日本国特許庁 JAPAN PATENT OFFICE

02.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月２５日

出願番号
Application Number: 特願２００３－３９４７０９

[ST. 10/C]: [ＪＰ２００３－３９４７０９]

出願人
Applicant(s): 松下電器産業株式会社

２００５年 １月１３日

特許庁長官
Commissioner,
Japan Patent Office 小川洋

【書類名】　特許願
【整理番号】　2048150053
【提出日】　平成15年11月25日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　石原　秀志
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、
前記端末装置は、
複数の認証用データを格納する格納部と、
前記付帯情報を受信する受信部と、
前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、
比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする認証システム。
【請求項２】
前記複数の認証用データのうち少なくとも１つは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも１つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする請求項１記載の認証システム。
【請求項３】
前記端末装置はさらに、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、
前記読出装置はさらに、前記部分認証用データを受信する受信部を備えることを特徴とする請求項２記載の認証システム。
【請求項４】
前記読出装置はさらに、
認証用データの付帯情報を格納する格納部と、
前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、
データを送信する送信部を備え、
比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項１記載の認証システム。
【請求項５】
前記読出装置はさらに、
認証用データを格納する格納部と、
前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、
データを送信する送信部を備え、
比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項１記載の認証システム。
【請求項６】
前記記録媒体が、認証用データ自身も記録することを特徴とする請求項１記載の認証システム。
【請求項７】
前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項１記載の認証システム。
【請求項８】
認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、
前記端末装置は、
１つの認証用データを格納する格納部と、
前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、

比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、

前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする認証システム。

【請求項９】

前記端末装置はさらに、

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、

前記読出装置はさらに、前記部分認証用データを受信する受信部を備えることを特徴とする請求項８記載の認証システム。

【請求項１０】

前記読出装置はさらに、

認証用データの付帯情報を格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項８記載の認証システム。

【請求項１１】

前記読出装置はさらに、

認証用データを格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項８記載の認証システム。

【請求項１２】

前記記録媒体が、認証用データ自身も記録することを特徴とする請求項８記載の認証システム。

【請求項１３】

前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項８記載の認証システム。

【請求項１４】

記録媒体を利用する端末装置であって、

複数の認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、

比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする端末装置。

【請求項１５】

前記複数の認証用データのうち少なくとも１つは、前記端末装置自身の有効性を読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも１つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする請求項１４記載の端末装置。

【請求項１６】

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする請求項１５記載の端末装置。

【請求項１７】

記録媒体を利用する端末装置であって、

１つの認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、

比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、

前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする端末装置。

【請求項１８】

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする請求項１７記載の端末装置。

【請求項１９】

記録媒体から付帯情報を読み出す読出装置であって、

認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、

比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部と、

前記端末装置から部分認証用データを受信する受信部と、

前記受信した部分認証用データを検証する検証部を備えることを特徴とする読出装置。

【請求項２０】

前記読出装置はさらに、

認証用データの付帯情報を格納する格納部と、

記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項１９記載の読出装置。

【請求項２１】

前記読出装置はさらに、

認証用データを格納する格納部と、

記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項１９記載の読出装置。

【請求項２２】

認証用データの付帯情報を記録する記録媒体であって、

端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して

認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、

前記記録媒体は、前記端末装置により利用されることを特徴とする記録媒体。

【請求項２３】

認証用データであって、

前記認証用データは、端末装置の有効性を示すデータと、読出装置の有効性を示すデータが一体化されていることを特徴とする認証用データ。

【請求項２４】

前記認証用データは、前記端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項２３記載の認証用データ。

【請求項２５】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする請求項２３記載の認証用データ。

【請求項２６】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項２３記載の認証用データ。

【請求項２７】

前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする請求項２４記載の認証用データ。

【請求項２８】

認証用データであって、

前記認証用データは、有効であることを示すデータ、無効であること示すデータ、有効である区間を示すデータ、無効である区間を示すデータが混在し、少なくとも２つ以上の組み合わせにより構成されることを特徴とする認証用データ。

【請求項２９】

前記認証用データは、区間を示すデータの場合、区間であることを示すフラグが存在することを特徴とする請求項２８記載の認証用データ。

【請求項３０】

前記認証用データは、端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項２８記載の認証用データ。

【請求項３１】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする請求項２８記載の認証用データ。

【請求項３２】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項２８記載の認証用データ。

【請求項３３】

前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする請求項２８記載の認証用データ。

【書類名】明細書
【発明の名称】認証システム、端末装置、読出装置、記録媒体、及び認証用データ
【技術分野】
【０００１】
本発明は、公開鍵暗号を利用した認証システムに関するものであり、公開鍵証明書の有効性を判定するためのリストを含む認証システムに関する。
【背景技術】
【０００２】
近年、インターネットの急速な広がりにより、インターネットをその通信の基盤とするシステムも増加している。例えば、インターネットを介して物品の売買を行う電子商取引もその１つである。このような、インターネットを通信の基盤とするシステムにおいては、通信相手がシステムの正当な参加者であることを確認することが必須となる。これを認証という。通信相手としては人間が機器を操作している場合や、機器が予め決められた手順で処理を行う場合があるが、以下ではこの両者を含めて機器という。そして通信相手を認証することを機器認証という。なお、機器が正当性、すなわち自分がシステムの正当な参加者であることを示すことを「証明する」といい、相手の正当性を確認することを「検証する」という。認証とは証明と検証の両方を含む言葉とする。
【０００３】
また、暗号技術には共通鍵暗号と公開鍵暗号がある。共通鍵暗号は暗号化のための鍵と復号のための鍵が同じ物である。一方、公開鍵暗号は暗号化のための鍵と復号のための鍵が異なるものである。認証を行うには公開鍵暗号を用いる方が望ましい。なぜならば、共通鍵暗号を用いた認証においては，検証者は証明者と同じ秘密を持つので、これ以降、検証者が証明者になりすます危険性がある。いわゆるパスワード方式はこれに該当する。公開鍵暗号を用いた認証においては，証明者は公開鍵暗号の秘密鍵を用いて証明し、検証者はその秘密鍵に対する公開鍵を用いて検証するのであり、公開鍵から秘密鍵は作成できないようになっているので、認証が終わった後で、検証者が証明者になりすますことができないからである。
【０００４】
なお、公開鍵暗号技術において、秘密鍵を用いて処理を行うことを署名といい、対応する公開鍵を用いてその署名の正当性を確認することを検証するという。
公開鍵暗号を用いた相手認証処理の例として、第１の機器が第２の機器にチャレンジデータとして乱数データを送信し、続いて、第２の機器がその乱数データに対して自分の秘密鍵で署名を行って第１の機器にレスポンスデータを返信し、最後に、返信されてきた署名文に対して、第１の機器が第２の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが当該システム内で有効なものであることが前提となる。
【０００５】
このために、当該システムにおいて認証局（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ：以下、ＣＡ）と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、そのデータに対する認証局の電子署名の正しさを確認し、さらに相手機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、システムから排除され，正当ではないとされる機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ：以下、ＣＲＬ）として発行される。
【０００６】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器の公開鍵証明書を入手し、入手した公開鍵証明書がＣＲＬに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な相手機器との取引を回避することができる。なお、ＣＲＬの形式、実現例等は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。そのＣＲＬの実現例の一つとしては、特許文献１が開示されており、ＣＲＬ形式の一例としては、非特許文献１にＩＳＯ／ＩＥＣ／ＩＴＵが定めたＸ．５０９標準で定義されるＣＲＬ形式（データ構造）が開示されている。

【特許文献１】特開２００３－１１５８３８号公報
【特許文献２】特開２００２－２８１０１３号公報
【非特許文献１】山田慎一郎訳、「ディジタル署名と暗号技術」、ピアソン・エデュケーション
【非特許文献２】池野信一、小山謙二、「現代暗号理論」、電子通信学会

【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、前記従来の構成で相手の公開鍵証明書の有効性を判定する場合、当該リストの入手経路の一つとしてネットワーク接続が考えられるが、機器の利用ユーザによりネットワークが遮断されていると、リストが正しく入手／更新されない可能性がある。これは、自身の通信相手が有効か無効かを判断するためだけに用いられるリストに対しては、その入手／更新に対して強制力が働かないためである。
【０００８】
本発明は、前記従来の課題を解決するもので、リストのアップデートを強制化可能な認証システムの提供を目的とする。
【課題を解決するための手段】
【０００９】
本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする。
【００１０】
また、本発明は、前記認証システムであって、前記複数の認証用データのうち少なくとも１つは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも１つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする。
また、本発明は、前記認証システムであって、前記端末装置は、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置は、前記部分認証用データを受信する受信部を備えることを特徴とする。
【００１１】
また、本発明は、前記認証システムであって、前記読出装置は、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。
【００１２】
また、本発明は、前記認証システムであって、前記読出装置は、認証用データを格納す

る格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【００１３】

また、本発明は、前記認証システムであって、前記記録媒体が、認証用データ自身も記録することを特徴とする。

また、本発明は、前記認証システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

また、本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、前記端末装置は、１つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする。

【００１４】

また、本発明は、前記認証システムであって、前記端末装置は、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置は、前記部分認証用データを受信する受信部を備えることを特徴とする。

また、本発明は、前記認証システムであって、前記読出装置は、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。

【００１５】

また、本発明は、前記認証システムであって、前記読出装置は、認証用データを格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【００１６】

また、本発明は、前記認証システムであって、前記記録媒体が、認証用データ自身も記録することを特徴とする。

また、本発明は、前記認証システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

また、本発明は、記録媒体を利用する端末装置であって、前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする。

【００１７】

また、本発明は、前記端末装置であって、前記複数の認証用データのうち少なくとも１つは、前記端末装置自身の有効性を読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも１つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置自身の有効性を前記読出装置に

提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする。

【００１８】

また、本発明は、記録媒体を利用する端末装置であって、前記端末装置は、１つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする。

【００１９】

また、本発明は、前記端末装置であって、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする。

また、本発明は、記録媒体から付帯情報を読み出す読出装置であって、端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、前記読出装置は、前記端末装置から部分認証用データを受信する受信部と、前記受信した部分認証用データを検証する検証部を備えることを特徴とする。

【００２０】

また、本発明は、前記読出装置であって、前記読出装置は、認証用データの付帯情報を格納する格納部と、記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。

【００２１】

また、本発明は、前記読出装置であって、前記読出装置は、認証用データを格納する格納部と、記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【００２２】

また、本発明は、認証用データの付帯情報を記録する記録媒体であって、端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、前記記録媒体は、前記端末装置により利用されることを特徴とする。

【００２３】

また、本発明は、認証用データであって、前記認証用データは、端末装置の有効性を示すデータと、読出装置の有効性を示すデータが一体化されていることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【００２４】

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有

効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【００２５】

また、本発明は、前記認証用データであって、前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする。

また、本発明は、認証用データであって、前記認証用データは、有効であることを示すデータ、無効であること示すデータ、有効である区間を示すデータ、無効である区間を示すデータが混在し、少なくとも２つ以上の組み合わせにより構成されることを特徴とする。

【００２６】

また、本発明は、前記認証用データであって、前記認証用データは、区間を示すデータの場合、区間であることを示すフラグが存在することを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【００２７】

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【００２８】

また、本発明は、前記認証用データであって、前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする。

【発明の効果】

【００２９】

本発明によれば、再生装置が、自身が有効であることを示すリストを更新する際に、通信相手の読出装置が有効か無効か判断するためのリストも合わせて更新することで、再生装置における読出装置に関するリストの更新を強制化させることができる。これは、再生装置が、自身が有効であることを示すリストを更新しない場合、読出装置からのコンテンツの供給がストップされることから、再生装置によるリストの更新は必須となり、その更新と合わせて読出装置のリストを更新することにより実現できる。

【００３０】

また、本発明によれば、再生装置が、自身の有効性を示すリストと、通信相手である読出装置の有効性を判断するためのリストを保持することから、これら２つのリストを１つにして、自身の有効性を示すリストの更新が、通信相手の有効性を判断するリストの更新と等価になるようにすることでリストの更新を強制化することができる。

【発明を実施するための最良の形態】

【００３１】

以下、本発明の実施の形態について、図面を参照しながら説明する。図１は、本発明に係る認証システムの全体構成を示すブロック図である。このシステムは、公開鍵の正当性を示す公開鍵証明書と、読出装置が保持する公開鍵証明書の有効性を示すリスト（以下、リストＤ）と、再生装置が保持する公開鍵証明書の有効性を示すリスト（以下、リストＨ）を発行する公開鍵証明書認証局（以下、ＣＡ）の端末装置１０１と、暗号化されたコンテンツ（以下、暗号化コンテンツ）を記録する記録媒体１０２と、前記記録媒体１０２から暗号化コンテンツを読み出す読出装置１０３と、前記読出装置１０３と認証を行い、前

記暗号化コンテンツを復号して再生する再生装置１０４からなる。

【００３２】

ここでは、読出装置の処理負荷を軽減することを目的として、再生装置がリストＤを検索して、通信相手である読出装置が保持する公開鍵証明書が有効か否かを判断し、さらに、同じく再生装置がリストＨを検索して、通信相手である読出装置に対して、自身が保持する公開鍵証明書が有効であることを示すリストＨの部分データを送信する形態とする。このような構成にすることで、読出装置は、再生装置から送られるリストＨの部分データのみを検証／確認するだけで再生装置の有効性を判断することが可能となるため処理負荷の軽減につながる。

【００３３】

さらに、再生装置１０４は、自身の有効性を示すリストＨの更新が必要な場合、ネットワークを介して認証局端末装置１０１に接続して、認証局端末装置１０１から更新版のリストＨを取得する。その時、リストＤも同様に取得する。

また、読出装置１０３と再生装置１０４は、汎用の通信路で接続されており、一方が他方を認証する片方向認証、あるいは両者が互いに認証し合う相互認証を実施した後、認証結果がＯＫであれば、読出装置１０３は、暗号化コンテンツを再生装置１０４へ送信し、再生装置１０４がコンテンツの再生を行う。ここで、汎用の通信路とは、その仕様が公開されているため、通信路上のデータ盗聴、改ざん、差し替えなどの危険に晒される安全でない通信路のことである。

【００３４】

次に、図２、及び図３に、読出装置の有効性を判断するためのリストＤの構成、並びに再生装置の有効性を判断するためのリストＨの構成の一例を示す。

図２は、読出装置が保持する公開鍵証明書のうち、ＩＤ＝１、ＩＤ＝６、ＩＤ＝７、ＩＤ＝１５の４つの公開鍵証明書が無効化されている場合のリストＤの例を示している。リストＤは、当該リストのバージョン番号を格納するバージョン番号フィールド２０１と、無効化すべき公開鍵証明書のＩＤを格納する無効化ＩＤフィールド２０２と、前記記フィールドの正当性を検証するための署名を格納する署名フィールド２０３により構成される。図２の例では、バージョン番号フィールド２０１には、バージョン番号「０００３」が格納され、無効化ＩＤフィールド２０２には、無効化すべきＩＤ「０００１」、「０００６」、「０００７」、「００１５」が格納され、署名フィールド２０３には、前記フィールドの各データが正しいことを示す署名（全フィールドのデータを連結した値に対してＣＡが付与した署名）が格納される。ただし、記号「||」は、データを連結することを意味する記号として用い、関数Ｓｉｇ（Ｘ，Ｙ）は、データＹに対して、鍵データＸを用いて署名生成を行う関数として用いる。また、ＳＫ＿ＣＡはＣＡだけが保持する署名生成に利用する秘密鍵のことである。

【００３５】

なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには無効化ＩＤフィールドがなく、検証時に署名から無効化ＩＤを生成する形態であってもよい。

【００３６】

図３は、再生装置が保持する公開鍵証明書のうち、ＩＤ＝１、ＩＤ＝５、ＩＤ＝９、ＩＤ＝１３～１６の７つの公開鍵証明書が無効化されている場合のリストＨの例を示している。リストＨは、当該リストのバージョン番号を格納するバージョン番号フィールド３０１と、有効な公開鍵証明書の区間の先頭ＩＤと終端ＩＤを格納する有効ＩＤフィールド３０２～３０９と、前記区間のそれぞれの正当性を検証するための署名を格納する署名フィールド３１０～３１３により構成される。図３の例では、バージョン番号フィールド３０１には、バージョン番号「０００３」が格納され、有効ＩＤフィールド３０２～３０９には、有効なＩＤの先頭、及び終端「０００２」、「０００４」、「０００６」、「０００

８」、「００１０」、「００１２」、「００１７」、「９９９９」が格納され、署名フィールド３１０～３１３には、前記ＩＤフィールドの区間が正しいことを示す署名（各区間の先頭、及び終端ＩＤに対してＣＡが付与した署名）が格納される。

【００３７】

なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには有効ＩＤフィールドがなく、検証時に署名から有効ＩＤの先頭、及び終端を生成する形態であってもよい。

【００３８】

（実施の形態１）

図４は、本発明の実施の形態１における、読出装置４００と再生装置４２０が相互認証を実行する場合の読出装置４００、並びに再生装置４２０の機能を示す機能ブロック図である。

読出装置４００は、ＣＡの公開鍵を格納するＣＡ公開鍵格納部４０１と、前記ＣＡの公開鍵を用いて、再生装置４２０から受信した部分リスト、及び証明書に対してＣＡが付与した署名の正当性を検証する、並びに受信した部分リストと証明書から当該証明書が有効であるか否かを検証する検証部４０２と、自身の証明書を格納する証明書格納部４０３と、前記自身の証明書を再生装置４２０へ送信する証明書送信部４０４と、読出装置４００と再生装置４２０を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ：ＳＡＣ）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部４０５と、記録媒体４５０に記録されている暗号化コンテンツ鍵を前記処理で共有した鍵（セッション鍵）で暗号化する暗号化部４０６を備える。

【００３９】

また、再生装置４２０は、自身の証明書を格納する証明書格納部４２１と、自身の証明書の有効性を示すリストＨの最新版を格納する最新リスト格納部４２２と、前記読出装置４００を経由して記録媒体４５０に記録されているリストＤ、かつリストＨのバージョン番号を受信して、前記最新リスト格納部４２２に格納するリストＨのバージョン番号と新旧を比較し、前記最新リスト格納部に格納するリストＨが古い場合に、外部ネットワークとの接続を促し、外部から最新版のリストＨを入手して、前記最新リスト格納部に格納するリストＨを更新する比較／更新部４２３と、前記証明書格納部４２１に格納する証明書と、前記最新リスト格納部４２２に格納するリストＨから、該当するＩＤの区間、バージョン番号、それらに対する署名からなる部分リストを抽出して、抽出した部分リストと証明書を読出装置４００へ送信する証明書／部分リスト送信部４２４と、ＣＡの公開鍵を格納するＣＡ公開鍵格納部４２５と、読出装置４００の有効性を示すリストＤの最新版を格納する最新リスト格納部４２６と、前記ＣＡの公開鍵を用いて、読出装置４００から受信した証明書に対してＣＡが付与した署名の正当性を検証する、並びに受信した証明書と前記最新リスト格納部４２６に格納する最新版のリストＤから当該証明書が有効であるか否かを検証する検証部４２７と、再生装置４２０と読出装置４００を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ：ＳＡＣ）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部４２８と、読出装置４００から受信した２重暗号化されたコンテンツ鍵を前記処理で共有した鍵（セッション鍵）で復号する復号部４２９と、再生装置４２０が保持するデバイス鍵を格納するデバイス鍵格納部４３０と、読出装置４００を経由して記録媒体４５０に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部４３１と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部４３２と、読出装置４００を経由して記録媒体４５０に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部４３３を備える。

【００４０】
また、記録媒体４５０には、暗号化メディア鍵４５１、リストＤ、かつリストＨのバージョン番号４５２、暗号化コンテンツ鍵４５３、暗号化コンテンツ４５４が記録されている。
なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献２が開示されている。
【００４１】
次に、記録媒体４５０に記録される各種データのデータ形式について、図５を用いて説明する。
記録媒体４５０は、暗号化メディア鍵を記録する暗号化メディア鍵記録領域４５１と、最新リストのバージョン番号を記録するバージョン番号記録領域４５２と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域４５３と、暗号化コンテンツを記録する暗号化コンテンツ記録領域４５４を備える。
【００４２】
最新リストのバージョン番号は、図５の例では「０００３」である。
暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵（ＤＫ）ではメディア鍵（Ｋｍ）を暗号化して、メディア鍵を与えない装置が持つデバイス鍵（ＤＫ）ではメディア鍵とは全く無関係なダミーデータを暗号化する。図８は、ＤＫ３を持つ装置と、ＤＫ１０を持つ装置に対してはメディア鍵を与えない場合の例を示している。
【００４３】
暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。
次に、図６～図９を用いて、読出装置４００と再生装置４２０の動作について説明する。
Ｓ６０１：再生装置４２０は、読出装置４００を経由して記録媒体４５０からバージョン番号を受信する。
【００４４】
Ｓ６０２：再生装置４２０は、受信したバージョン番号と、自身が保持するリストＨのバージョン番号を比較して、保持するリストＨのバージョン番号が受信したバージョン番号よりも新しいか否かを判断する。
Ｓ６０３：Ｓ６０２で判断した結果、新しければＳ６０６へ、古ければＳ６０４の処理へ移る。
【００４５】
Ｓ６０４：再生装置４２０は、ネットワークを介して外部と接続して、ＣＡから最新のリストＨ、並びにリストＤを入手する。
Ｓ６０５：Ｓ６０４で入手した最新のリストをそれぞれ格納する。
Ｓ６０６：再生装置４２０は、自身が保持するリストＨと、同じく自身が保持する証明書から該当する部分リストを抽出して、証明書と共に読出装置へ送信する。例えば、証明書ＩＤとして「０００７」を持つ再生装置４２０が、図３に示すリストＨを保持している場合、自身の有効性を示す３０４、３０５、及び３１１を部分リストとして抽出する。
【００４６】
Ｓ７０１：読出装置４００は、再生装置４２０から受信した部分リスト、及び証明書に対して、まず、ＣＡの公開鍵を利用してそれぞれに付与されている署名の検証を行う。さらに、部分リストが示す証明書の有効ＩＤと、受信した再生装置４２０の証明書のＩＤを比較して、当該証明書が有効か否かを検証する。
Ｓ７０２：Ｓ７０１で検証した結果、検証結果が全てＯＫであればＳ７０３へ、検証結果が１つでもＮＧであれば処理を中止する。
【００４７】

Ｓ７０３：読出装置４００は、保持する自身の証明書を再生装置４２０へ送信する。
Ｓ８０１：再生装置４２０は、読出装置４００から受信した証明書に対して、まず、ＣＡの公開鍵を利用して付与されている署名の検証を行う。さらに、自身が保持するリストＤと、受信した読出装置４００の証明書のＩＤを比較して、当該証明書が有効か否かを検証する。

【００４８】

Ｓ８０２：Ｓ８０１で検証した結果、検証結果が全てＯＫであればＳ８０３へ、検証結果が１つでもＮＧであれば処理を中止する。
Ｓ８０３／Ｓ８０４：読出装置４００と再生装置４２０の間では、両者の公開鍵暗号化処理部が動作してＳＡＣを確立し、データの受け渡しはＳＡＣを介して安全に行われる。このＳＡＣの実現方法については、後に詳細を述べる。ＳＡＣ処理の結果として、両者はセッション鍵を共有する。

【００４９】

Ｓ９０１：読出装置４００は、Ｓ８０４で生成したセッション鍵を用いて、記録媒体４５０に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置４２０へ送信する。
Ｓ９０２：再生装置４２０は、読出装置４００から受信した２重暗号化されたコンテンツ鍵を、Ｓ８０３で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【００５０】

Ｓ９０３：再生装置４２０は、読出装置４００を経由して記録媒体４５０から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、Ｓ９０２で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。
Ｓ９０４：再生装置４２０は、読出装置４００を経由して記録媒体４５０から暗号化コンテンツを受信して、Ｓ９０３で得たコンテンツ鍵で復号してコンテンツを得る。

【００５１】

以上に示したように、再生装置の保持するリストＨが古い場合、リストＨを更新しなければ、再生装置は読出装置によって認証されないため、再生装置のリストＨの更新を促す／強制化することができる。その際に、リストＤも合わせて更新することにより、本来強制力の働かないリストＤの更新も行うことが可能となる。
次に、読出装置４００と再生装置４２０との間で設定されるＳＡＣの実現方法について図１０を用いて説明する。ただし、Ｓｉｇｎ（）を署名生成関数、Ｖｅｒｉ（）を署名検証関数、Ｇｅｎ（）を鍵生成関数とし、Ｙをそのシステム固有のシステムパラメータとする。また、鍵生成関数Ｇｅｎ（）は、Ｇｅｎ（ｘ，Ｇｅｎ（ｙ，ｚ））＝Ｇｅｎ（ｙ，Ｇｅｎ（ｘ，ｚ））の関係を満たすものとする。なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、非特許文献２に、ディフィーヘルマン（ＤＨ）型公開鍵配送法が開示されている。

【００５２】

Ｓ１００１：読出装置Ａは、ＣＡが発行した証明書Ｃｅｒｔ＿Ａを再生装置Ｂに送信する。ここでは、証明書の構成要素は、Ａの公開鍵ＰＫ＿Ａ、ＡのＩＤ（ＩＤ＿Ａ）、それらに対するＣＡの署名Ｓｉｇ＿ＣＡとしている。
Ｓ１００２：再生装置Ｂは、ＣＡの公開鍵Ｐ＿ＣＡを用いてＣｅｒｔ＿Ａに付与されている署名Ｓｉｇ＿ＣＡが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。さらに、再生装置Ｂは、読出装置ＡのＩＤ（ＩＤ＿Ａ）が、ＣＲＬに登録されているか否かを確認する。登録されている場合も、ＳＡＣの設定処理を終了する。

【００５３】

Ｓ１００３：再生装置Ｂは、ＣＡが発行した証明書Ｃｅｒｔ＿Ｂを読出装置Ａに送信する。ここでは、証明書の構成要素は、Ｂの公開鍵ＰＫ＿Ｂ、ＢのＩＤ（ＩＤ＿Ｂ）、それらに対するＣＡの署名Ｓｉｇ＿ＣＡとしている。
Ｓ１００４：読出装置Ａは、ＣＡの公開鍵Ｐ＿ＣＡを用いてＣｅｒｔ＿Ｂに付与されて

いる署名Ｓｉｇ＿ＣＡが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。さらに、読出装置Ａは、再生装置ＢのＩＤ（ＩＤ＿Ｂ）が、ＣＲＬに登録されているか否かを確認する。登録されている場合も、ＳＡＣの設定処理を終了する。

【００５４】

Ｓ１００５：読出装置Ａは、乱数Ｃｈａ＿Ａを生成して、再生装置Ｂに送信する。

Ｓ１００６：再生装置Ｂは、受信したＣｈａ＿Ａに対して、自身の秘密鍵ＳＫ＿Ｂで署名Ｓｉｇ＿Ｂを生成して、読出装置Ａに送信する。

Ｓ１００７：読出装置Ａは、Ｓ１００３で受信した再生装置Ｂの公開鍵ＰＫ＿Ｂを用いて、Ｓｉｇ＿Ｂが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。

【００５５】

Ｓ１００８：再生装置Ｂは、乱数Ｃｈａ＿Ｂを生成して、読出装置Ａに送信する。

Ｓ１００９：読出装置Ａは、受信したＣｈａ＿Ｂに対して、自身の秘密鍵ＳＫ＿Ａで署名Ｓｉｇ＿Ａを生成して、再生装置Ｂに送信する。

Ｓ１０１０：再生装置Ｂは、Ｓ１００１で受信した読出装置Ａの公開鍵ＰＫ＿Ａを用いて、Ｓｉｇ＿Ａが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。

【００５６】

Ｓ１０１１：再生装置Ｂは、乱数ｂを生成し、Ｋｅｙ＿Ｂ＝Ｇｅｎ（ｂ，Ｙ）を計算して読出装置Ａに送信する。

Ｓ１０１２：読出装置Ａは、乱数ａを生成し、Ｋｅｙ＿Ａ＝Ｇｅｎ（ａ，Ｙ）を計算して再生装置Ｂに送信する。さらに、読出装置Ａは、両者で共有する鍵Ｋｅｙ＿ＡＢ＝Ｇｅｎ（ｂ，Ｋｅｙ＿Ａ）を算出する。

【００５７】

Ｓ１０１３：再生装置Ｂは、両者で共有する鍵Ｋｅｙ＿ＡＢ＝Ｇｅｎ（ａ，Ｋｅｙ＿Ｂ）を算出する。

（実施の形態２）

図１１は、本発明の実施の形態２における、読出装置１１００と再生装置１１２０が相互認証を実行する場合の読出装置１１００、並びに再生装置１１２０の機能を示す機能ブロック図である。

【００５８】

読出装置１１００は、ＣＡの公開鍵を格納するＣＡ公開鍵格納部１１０１と、前記ＣＡの公開鍵を用いて、再生装置１１２０から受信した部分リスト、及び証明書に対してＣＡが付与した署名の正当性を検証する、並びに受信した部分リストと証明書から当該証明書が有効であるか否かを検証する検証部１１０２と、自身の証明書を格納する証明書格納部１１０３と、前記自身の証明書を再生装置１１２０へ送信する証明書送信部１１０４と、読出装置１１００と再生装置１１２０を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ：ＳＡＣ）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部１１０５と、記録媒体１１５０に記録されている暗号化コンテンツ鍵を前記処理で共有した鍵（セッション鍵）で暗号化する暗号化部１１０６を備える。

【００５９】

また、再生装置１１２０は、自身の証明書を格納する証明書格納部１１２１と、自身の証明書、並びに読出装置の有効性を示すリストの最新版を格納する最新リスト格納部１１２２と、前記読出装置１１００を経由して記録媒体１１５０に記録されているリストのバージョン番号を受信して、前記最新リスト格納部１１２２に格納するリストのバージョン番号と新旧を比較し、前記最新リスト格納部に格納するリストが古い場合に、外部ネットワークとの接続を促し、外部から最新版のリストを入手して、前記最新リスト格納部に格納するリストを更新する比較／更新部１１２３と、前記証明書格納部１１２１に格納する

証明書と、前記最新リスト格納部１１２２に格納するリストから、該当するＩＤの区間、バージョン番号、それらに対する署名からなる部分リストを抽出して、抽出した部分リストと証明書を読出装置１１００へ送信する証明書／部分リスト送信部１１２４と、ＣＡの公開鍵を格納するＣＡ公開鍵格納部１１２５と、前記ＣＡの公開鍵を用いて、読出装置１１００から受信した証明書に対してＣＡが付与した署名の正当性を検証する、並びに受信した証明書と前記最新リスト格納部１１２６に格納する最新版のリストから当該証明書が有効であるか否かを検証する検証部１１２７と、再生装置１１２０と読出装置１１００を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Ｓｅｃｕｒｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｈａｎｎｅｌ：ＳＡＣ）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部１１２８と、読出装置１１００から受信した２重暗号化されたコンテンツ鍵を前記処理で共有した鍵（セッション鍵）で復号する復号部１１２９と、再生装置１１２０が保持するデバイス鍵を格納するデバイス鍵格納部１１３０と、読出装置１１００を経由して記録媒体１１５０に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部１１３１と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部１１3.2と、読出装置１１００を経由して記録媒体１１５０に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部１１３３を備える。

【００６０】

また、記録媒体１１５０には、暗号化メディア鍵１１５１、最新リストのバージョン番号１１５２、暗号化コンテンツ鍵１１５３、暗号化コンテンツ１１５４が記録されている。

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献２が開示されている。

【００６１】

次に、図１２にリストの一例を示す。図１２は、読出装置が保持する公開鍵証明書のうち、ＩＤ＝１、ＩＤ＝２の２つの公開鍵証明書が無効化されている場合、及び再生装置が保持する公開鍵証明書のうち、ＩＤ＝９、ＩＤ＝１３～１６の５つの公開鍵証明書が無効化されている場合のリストの例を示している。リストは、当該リストのバージョン番号を格納するバージョン番号フィールド１２０１と、読出装置の無効化すべき公開鍵証明書のＩＤを格納する無効化ＩＤフィールド１２０２～１２０３と、有効な公開鍵証明書の区間の先頭ＩＤと終端ＩＤを格納する有効ＩＤフィールド１２０４～１２０９と、前記区間のそれぞれの正当性を検証するための署名を格納する署名フィールド１２１０～１２１２と、リスト全体の正当性を検証するための署名を格納する署名フィールド１２１３により構成される。図１２の例では、バージョン番号フィールド１２０１には、バージョン番号「０００３」が格納され、無効化ＩＤフィールド１２０２～１２０３には、読出装置の無効化すべきＩＤ「０００１」、「０００２」が格納され、有効ＩＤフィールド１２０４～１２０９には、再生装置の有効なＩＤの先頭、及び終端「０００６」、「０００８」、「００１０」、「００１２」、「００１７」、「９９９９」が格納され、署名フィールド１２１０～１２１２には、前記有効ＩＤフィールドの区間が正しいことを示す署名（各区間の先頭、及び終端ＩＤに対してＣＡが付与した署名）が格納され、署名フィールド１２１３には、前記フィールドの各データが正しいことを示す署名（全フィールドのデータを連結した値に対してＣＡが付与した署名）が格納される。なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには無効化ＩＤフィールドがなく、検証時に署名から無効化ＩＤを生成する形態であってもよい。

【００６２】

次に、図１３～図１６を用いて、読出装置１１００と再生装置１１２０の動作について

説明する。
Ｓ１３０１：再生装置１１２０は、読出装置１１００を経由して記録媒体１１５０からバージョン番号を受信する。
Ｓ１３０２：再生装置１１２０は、受信したバージョン番号と、自身が保持するリストのバージョン番号を比較して、保持するリストのバージョン番号が受信したバージョン番号よりも新しいか否かを判断する。
【００６３】
Ｓ１３０３：Ｓ１３０２で判断した結果、新しいければＳ１３０６へ、古ければＳ１３０４の処理へ移る。
Ｓ１３０４：再生装置１１２０は、ネットワークを介して外部と接続して、ＣＡから最新のリストを入手する。
Ｓ１３０５：Ｓ１３０４で入手した最新のリストをそれぞれ格納する。
【００６４】
Ｓ１３０６：再生装置１１２０は、自身が保持するリストと、同じく自身が保持する証明書から該当する部分リストを抽出して、証明書と共に読出装置へ送信する。例えば、証明書ＩＤとして「０００７」を持つ再生装置１１２０が、図１２に示すリストを保持している場合、自身の有効性を示す１２０４、１２０５、及び１２１０を部分リストとして抽出する。
【００６５】
Ｓ１４０１：読出装置１１００は、再生装置１１２０から受信した部分リスト、及び証明書に対して、まず、ＣＡの公開鍵を利用してそれぞれに付与されている署名の検証を行う。さらに、部分リストが示す証明書の有効ＩＤと、受信した再生装置１１２０の証明書のＩＤを比較して、当該証明書が有効か否かを検証する。
Ｓ１４０２：Ｓ１４０１で検証した結果、検証結果が全てＯＫであればＳ１４０３へ、検証結果が１つでもＮＧであれば処理を中止する。
【００６６】
Ｓ１４０３：読出装置１１００は、保持する自身の証明書を再生装置１１２０へ送信する。
Ｓ１５０１：再生装置１１２０は、読出装置１１００から受信した証明書に対して、まず、ＣＡの公開鍵を利用して付与されている署名の検証を行う。さらに、自身が保持するリストと、受信した読出装置１１００の証明書のＩＤを比較して、当該証明書が有効か否かを検証する。
【００６７】
Ｓ１５０２：Ｓ１５０１で検証した結果、検証結果が全てＯＫであればＳ１５０３へ、検証結果が１つでもＮＧであれば処理を中止する。
Ｓ１５０３／Ｓ１５０４：読出装置１１００と再生装置１１２０の間では、両者の公開鍵暗号化処理部が動作してＳＡＣを確立し、データの受け渡しはＳＡＣを介して安全に行われる。このＳＡＣの実現方法については、後に詳細を述べる。ＳＡＣ処理の結果として、両者はセッション鍵を共有する。
【００６８】
Ｓ１６０１：読出装置１１００は、Ｓ１５０４で生成したセッション鍵を用いて、記録媒体１１５０に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置１１２０へ送信する。
Ｓ１６０２：再生装置１１２０は、読出装置１１００から受信した２重暗号化されたコンテンツ鍵を、Ｓ１５０３で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。
【００６９】
Ｓ１６０３：再生装置１１２０は、読出装置１１００を経由して記録媒体１１５０から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、Ｓ１６０２で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

Ｓ１６０４：再生装置１１２０は、読出装置１１００を経由して記録媒体１１５０から暗号化コンテンツを受信して、Ｓ１６０３で得たコンテンツ鍵で復号してコンテンツを得る。

【００７０】

（その他の変形例）

（１）本発明の実施の形態１では、無効化するＩＤ、及び有効なＩＤの区間でリストを構成する形態とし、実施の形態２では、無効化するＩＤ、及び有効なＩＤの区間で１つのリストを構成する形態としたが、本発明はその構成に限定されるものではない。例えば、図１７に示すように、１つのリスト内に無効化するＩＤを示すフィールド１７０２～１７０３、有効なＩＤを示すフィールド１７０４～１７０５、有効なＩＤの区間を示すフィールド１７０６～１７０７、あるいはそれらの組み合わせでリストを構成する形態であってもよい。

【００７１】

さらに、例えば、図１８に示すように、無効化するＩＤを示すフィールド１８０２～１８０４、１８０７に対しては、その先頭にビット「０」を付与し、複数の無効化するＩＤ（区間）を示す１８０５～１８０６には、その先頭にビット「１」を付与してリストを構成する形態であってもよい。

（２）本発明の実施の形態１、及び実施の形態２では、記録媒体には予め暗号化されたコンテンツが記録されているＤＶＤ－Ｖｉｄｅｏのようなプリレコーディッドメディアの形態としたが、本発明はその構成に限定されるものではない。例えば、ＤＶＤ－ＲＡＭのようなレコーダブルメディアであってもよい。その場合、実施の形態１、及び実施の形態２と同様に認証を実行した後で、暗号化されたコンテンツが記録媒体に記録される形態となる。さらにその場合は、実施の形態１、及び実施の形態２は、再生装置の代わりに記録装置により実現される。

【００７２】

（３）本発明の実施の形態１、及び実施の形態２では、記録媒体にはバージョン番号のみが記録されている形態としたが、本発明はその構成に限定されるものではない。例えば、記録媒体には、バージョン番号と共に、最新リストも記録されており、記録媒体に記録されている最新リストを利用して再生装置がリストを更新する構成であってもよい。

（４）実施の形態１、及び実施の形態２において、読出装置が、リストのバージョン番号を格納する格納部を有する構成であってもよい。この場合、読出装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、新しいバージョン番号を再生装置に送信する構成であってもよい。

【００７３】

さらに、読出装置が、リストのバージョン番号に加え、リスト自身を格納する格納部を有する構成であってもよい。この場合、読出装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、自身が保持するバージョン番号が新しければ、保持するバージョン番号、並びにリストを再生装置に送信する構成であってもよい。

【００７４】

（５）本発明の実施の形態１、及び実施の形態２では、認証に用いるデータ、及びコンテンツが記録媒体に記録される形態としたが、本発明はその構成に限定されるものではない。記録媒体の代わりに通信媒体を利用して、通信媒体を介して、認証に用いるデータ、及びコンテンツを受け渡しする構成であってもよい。また、記録媒体、並びに通信媒体を併用する形態であってもよい。

【００７５】

（６）本発明の実施の形態１、及び実施の形態２では、認証に用いるデータの保護にＣＡの署名を用いる形態としたが本発明はその構成に限定されるものではない。例えば、読出装置は読出装置専用の秘密鍵を保持し、再生装置は再生装置専用の秘密鍵を用いる構成として、認証に用いるデータには、各秘密鍵を利用して生成された認証子を付与する構成

であってもよい。

【００７６】

（７）実施の形態１、及び実施の形態２において、再生装置が、例えばＰＣにインストールされる再生用ソフトウェアであってもよい。あるいは、記録用ソフトウェアであってもよい。

【産業上の利用可能性】

【００７７】

本発明にかかる認証システムは、更新の強制力が働かない読出装置に対するリストの更新を、再生装置自身のリストの更新と同時に行う、あるいはリスト自身を一体化させることにより、効果的な認証を実現できるという効果を有し、公開鍵暗号を利用した認証システムにおいて有用である。

【図面の簡単な説明】

【００７８】

【図１】本発明に係る認証システムの全体構成を示すブロック図
【図２】本発明に係るリストの例を示す図
【図３】本発明に係るリストの例を示す図
【図４】本発明の実施の形態１における機能ブロック図
【図５】本発明の実施の形態１における記録媒体に記録されるデータの例を示す図
【図６】本発明の実施の形態１における動作を示す図
【図７】本発明の実施の形態１における動作を示す図
【図８】本発明の実施の形態１における動作を示す図
【図９】本発明の実施の形態１における動作を示す図
【図１０】本発明に係る相互認証の例を示す図
【図１１】本発明の実施の形態２における機能ブロック図
【図１２】本発明の実施の形態２に係るリストの例を示す図
【図１３】本発明の実施の形態２における動作を示す図
【図１４】本発明の実施の形態２における動作を示す図
【図１５】本発明の実施の形態２における動作を示す図
【図１６】本発明の実施の形態２における動作を示す図
【図１７】本発明に係るリストの例を示す図
【図１８】本発明に係るリストの例を示す図

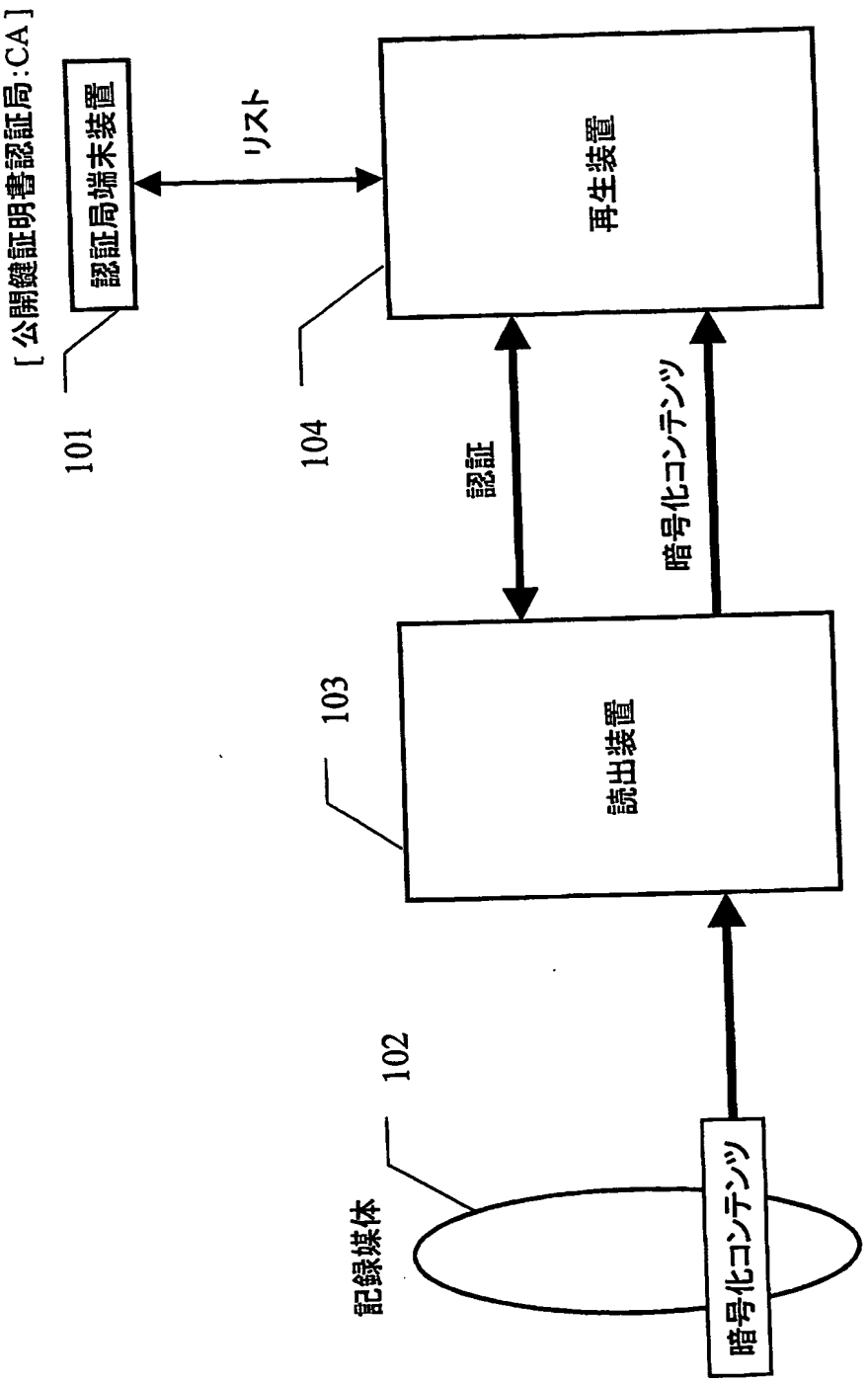
【符号の説明】

【００７９】

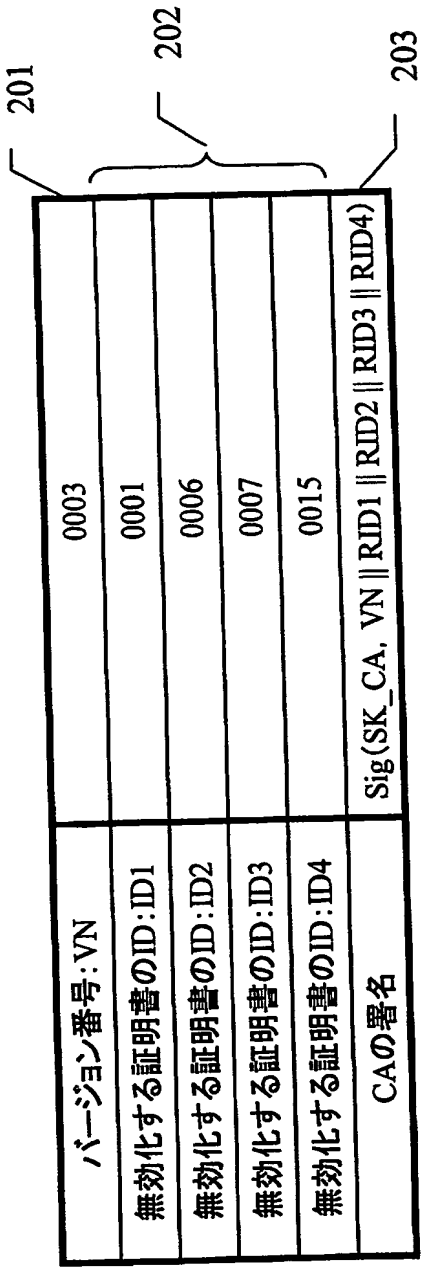
１０１　認証局端末装置
１０２、４５０、１１５０　記録媒体
１０３、４００、１１００　読出装置
１０４、４２０、１１２０　再生装置
４０１、４２５、１１０１、１１２５　ＣＡ公開鍵格納部
４０２、４２７、１１０２、１１２７　検証部
４０３、４２１、１１０３、１１２１　証明書格納部
４０４、１１０４　証明書送信部
４０５、４２８、１１０５、１１２８　公開鍵暗号処理部
４０６、１１０６　暗号化部
４２２、４２６、１１２２、１１２６　最新リスト格納部
４２３、１１２３　比較／更新部
４２４、１１２４　証明書／部分リスト送信部
４２９、４３１、４３２、４３３、１１２９、１１３１、１１３２、１１３３　復号部
４３０、１１３０　デバイス鍵格納部
４５１、１１５１　暗号化メディア鍵
４５２、１１５２　バージョン番号

４５３、１１５３　暗号化コンテンツ鍵
４５４、１１５４　暗号化コンテンツ

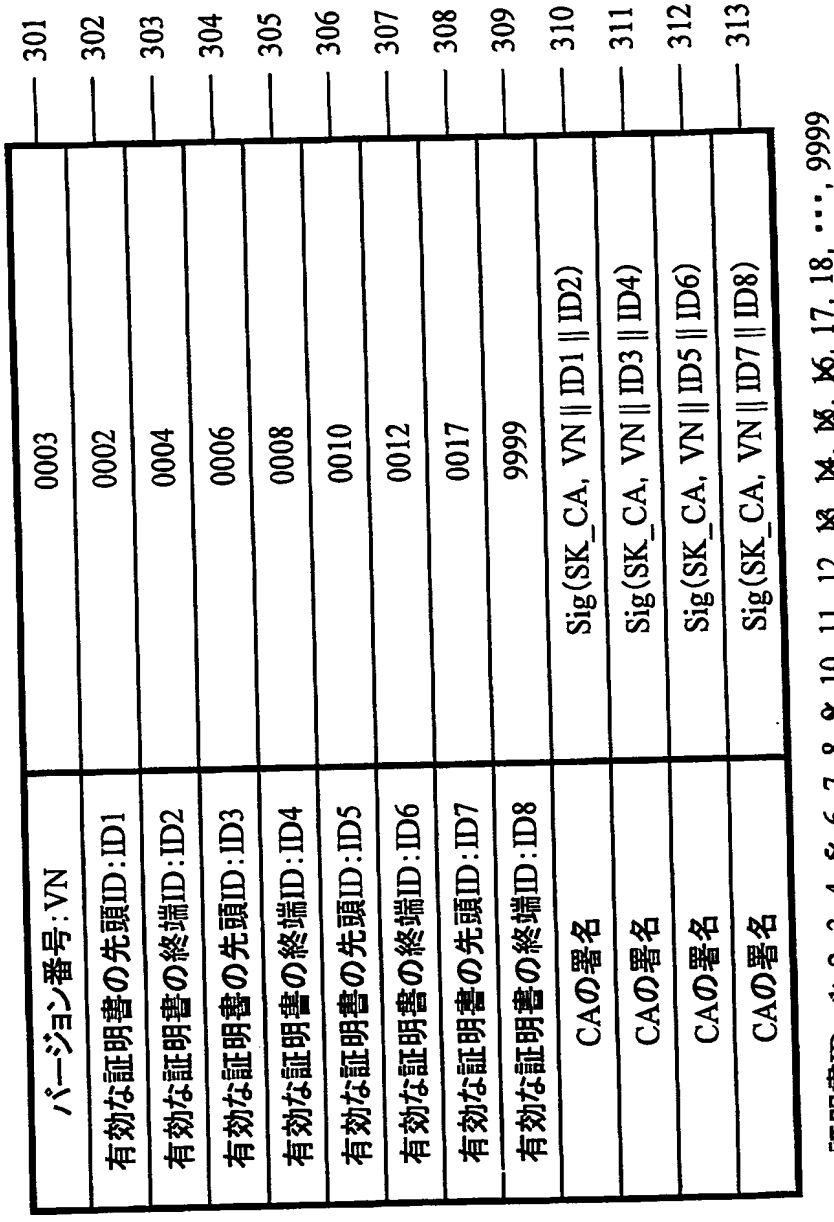
【書類名】図面
【図１】


［公開鍵証明書認証局:CA］
認証局端末装置
101
リスト
再生装置
104
認証
暗号化コンテンツ
103
読出装置
102
記録媒体
暗号化コンテンツ

【図２】


201
202
203
バージョン番号:VN
0003
無効化する証明書のID:ID1
0001
無効化する証明書のID:ID2
0006
無効化する証明書のID:ID3
0007
無効化する証明書のID:ID4
0015
CAの署名
Sig(SK_CA, VN || RID1 || RID2 || RID3 || RID4)
証明書ID：※, 2, 3, 4, 5, ※, ※, 8, 9, ・・・, ※, 16, ・・・
×：無効化すべきID

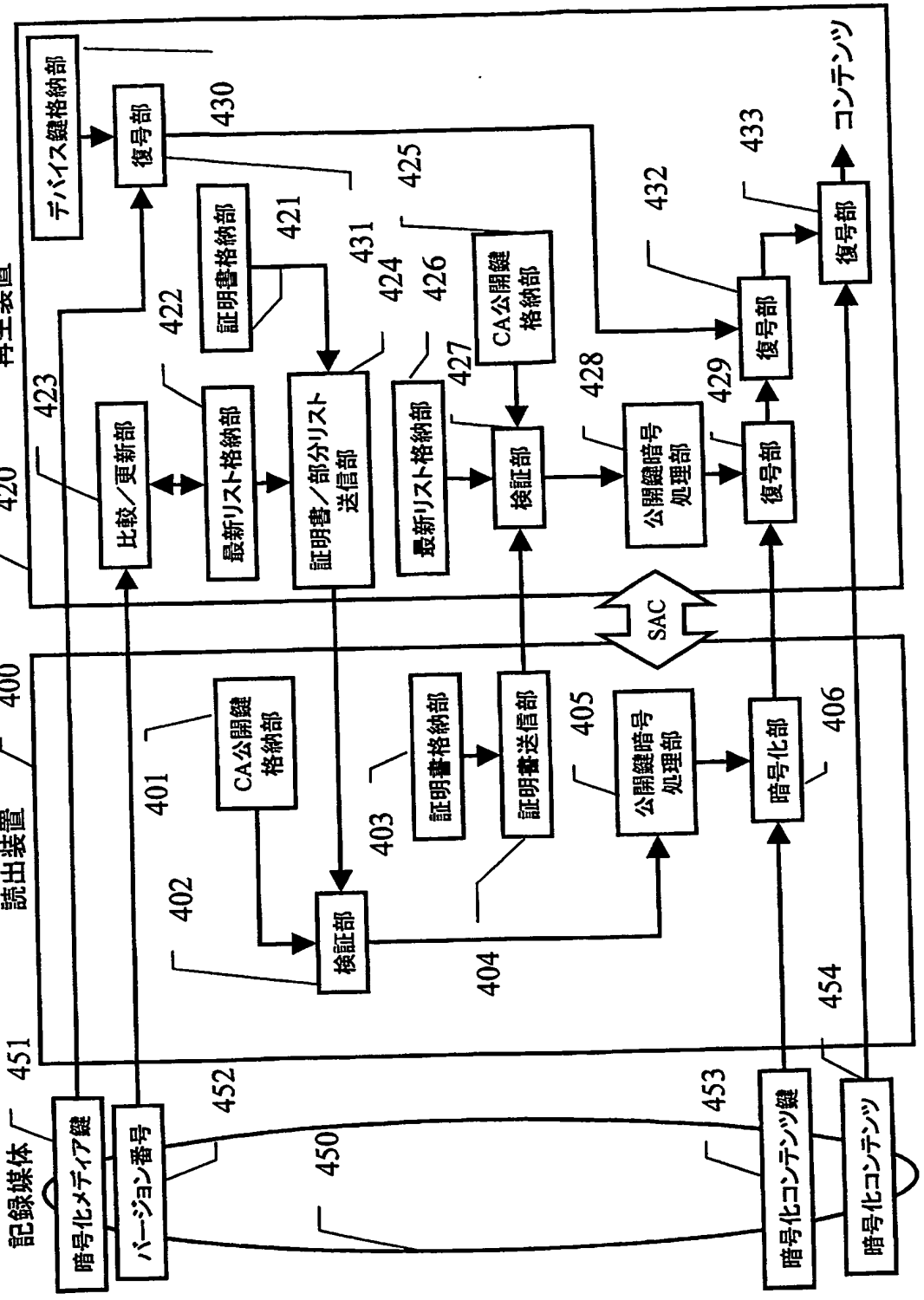
【図３】



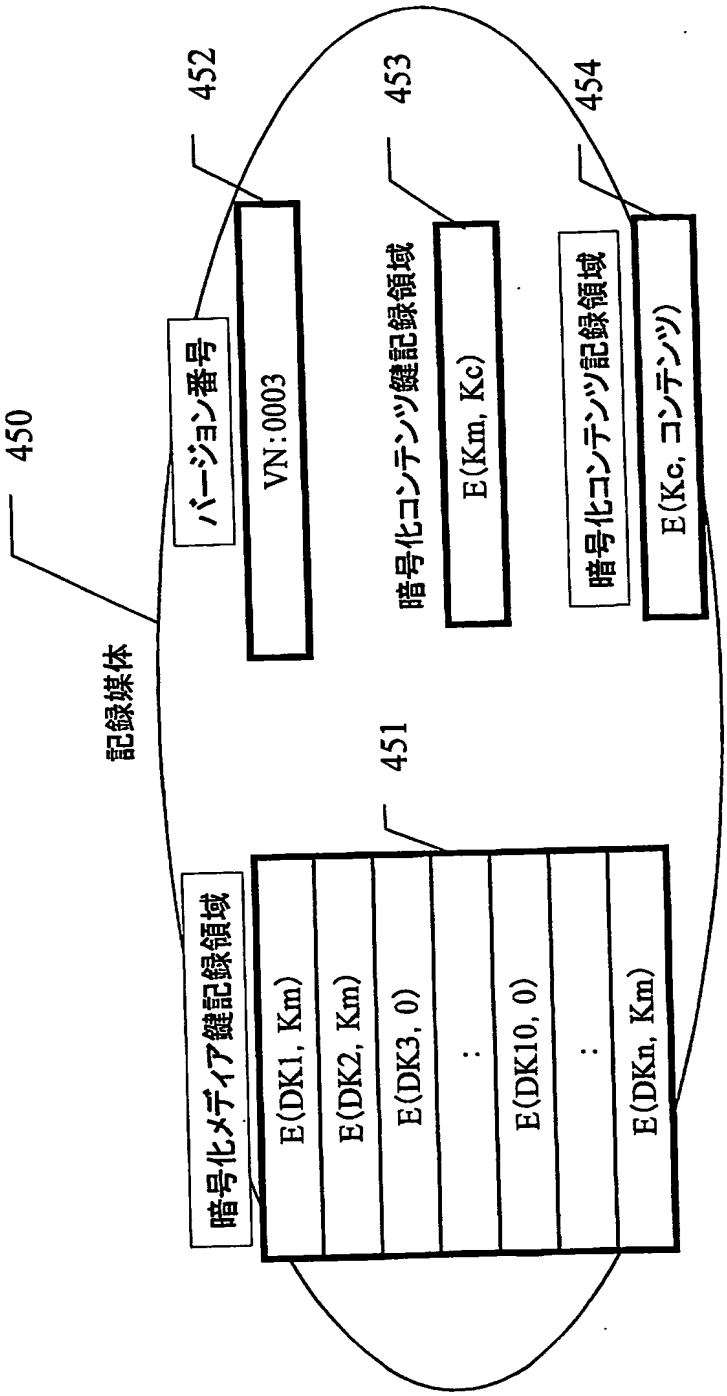
証明書ID：2, 3, 4, 6, 7, 8, 10, 11, 12, , , , , 17, 18, ･･･, 9999

×：無効化すべきID

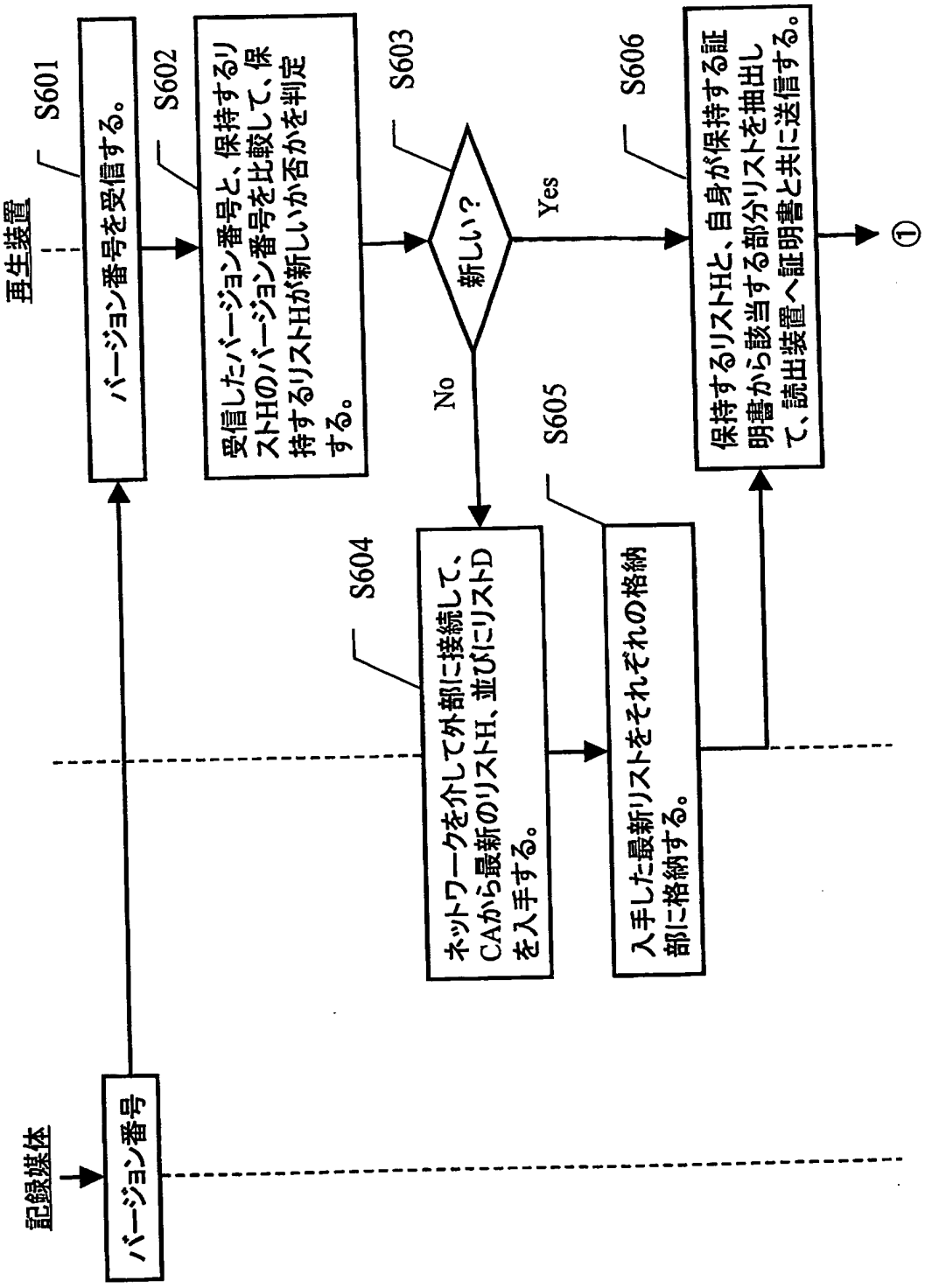
【図４】


記録媒体
暗号化メディア鍵
バージョン番号
暗号化コンテンツ鍵
暗号化コンテンツ
450
451
452
453
454
読出装置
400
CA公開鍵格納部
401
検証部
402
証明書格納部
403
404
証明書送信部
405
公開鍵暗号処理部
暗号化部
406
再生装置
420
比較／更新部
423
最新リスト格納部
422
証明書／部分リスト送信部
424
最新リスト格納部
427
検証部
428
公開鍵暗号処理部
429
復号部
復号部
復号部
コンテンツ
433
CA公開鍵格納部
426
432
証明書格納部
421
431
デバイス鍵格納部
復号部
430
425
SAC

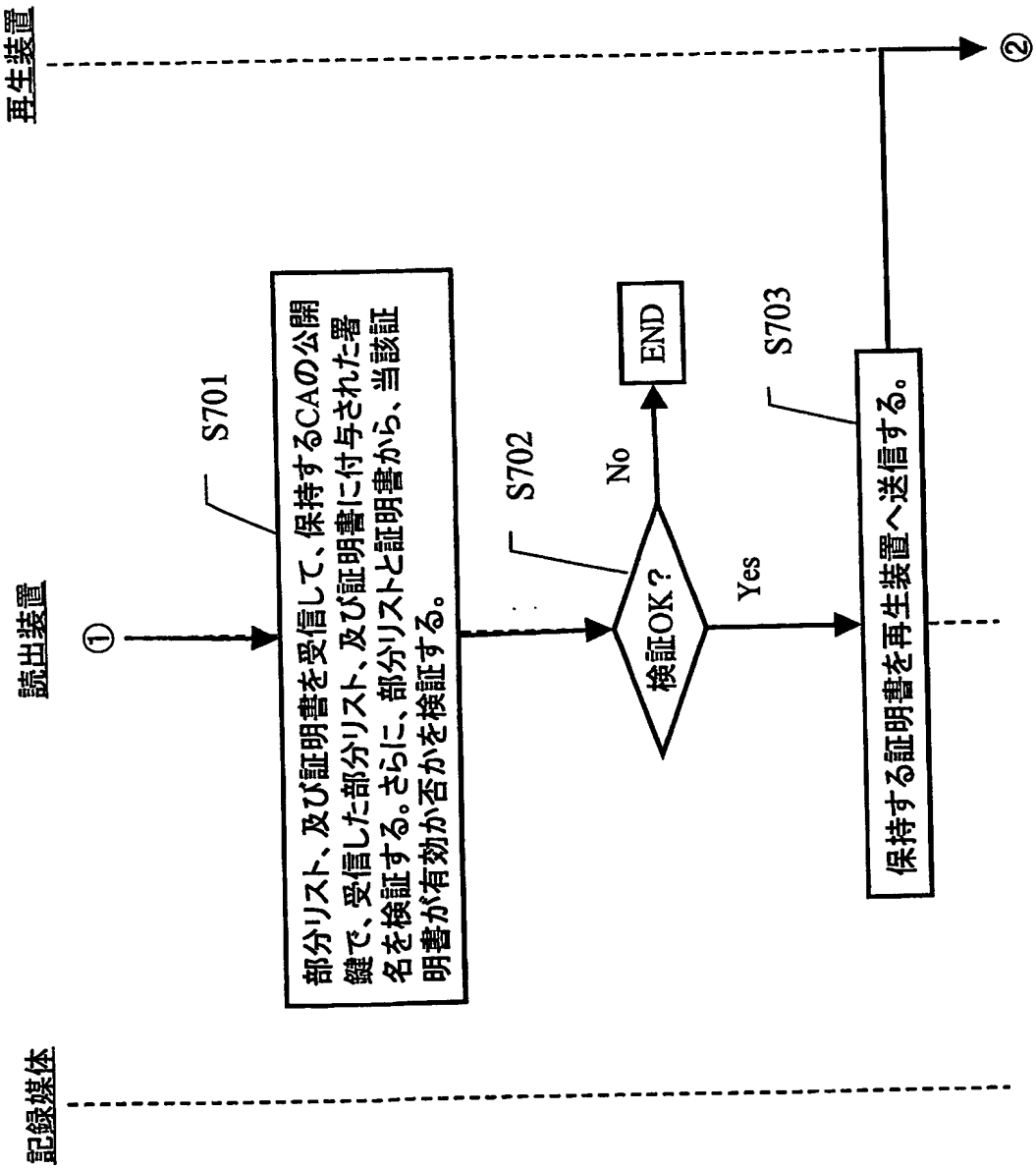
【図５】


450
記録媒体
452
453
454
451
バージョン番号
VN:0003
暗号化コンテンツ鍵記録領域
E(Km, Kc)
暗号化コンテンツ記録領域
E(Kc, コンテンツ)
暗号化メディア鍵記録領域
E(DK1, Km)
E(DK2, Km)
E(DK3, 0)
:
E(DK10, 0)
:
E(DKn, Km)

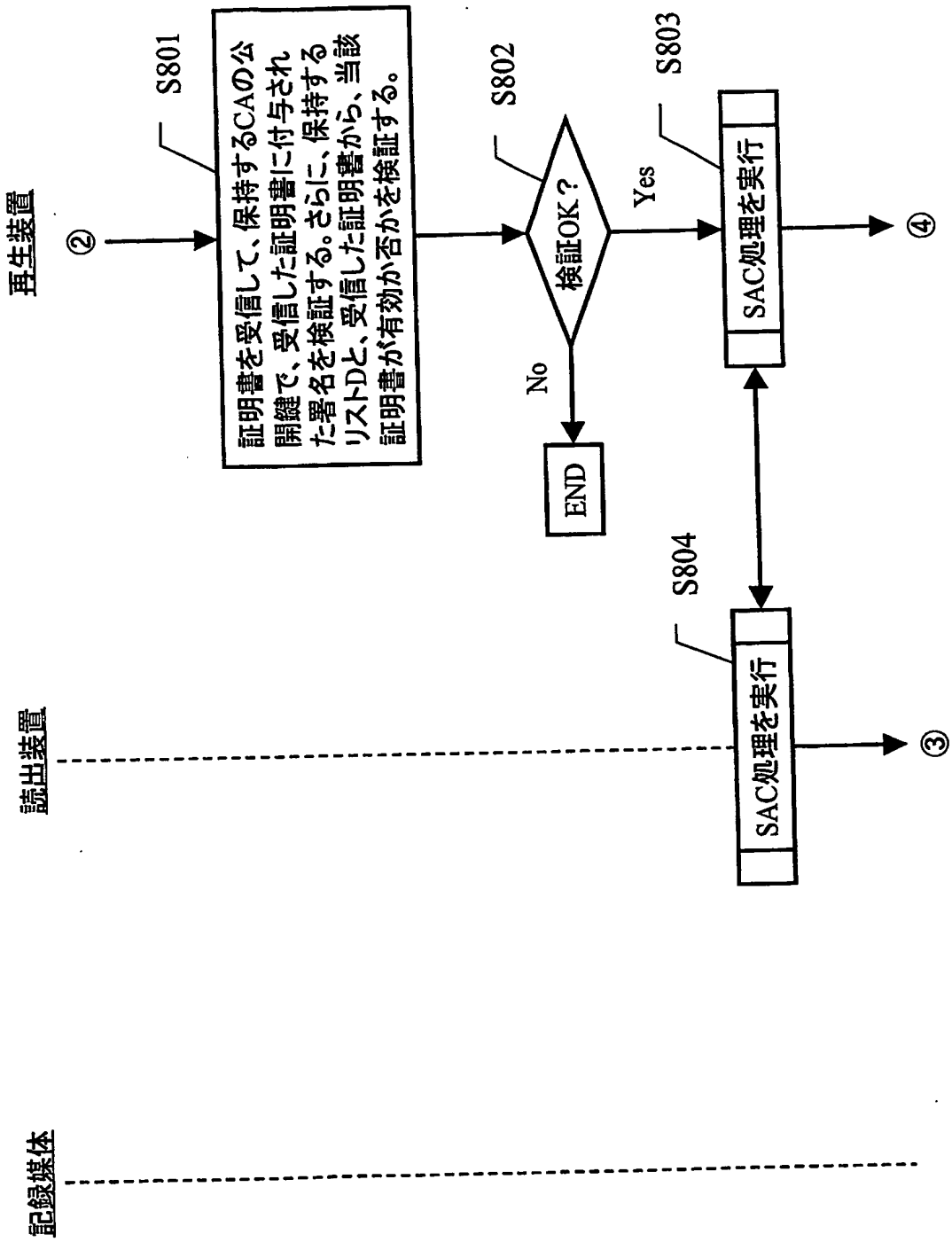
【図６】


記録媒体
バージョン番号
再生装置
バージョン番号を受信する。
S601
受信したバージョン番号と、保持するリストHのバージョン番号を比較して、保持するリストHが新しいか否かを判定する。
S602
新しい？
S603
Yes
No
保持するリストHと、自身が保持する証明書から該当する部分リストを抽出して、読出装置へ証明書と共に送信する。
S606
①
ネットワークを介して外部に接続して、CAから最新のリストH、並びにリストDを入手する。
S604
入手した最新リストをそれぞれの格納部に格納する。
S605

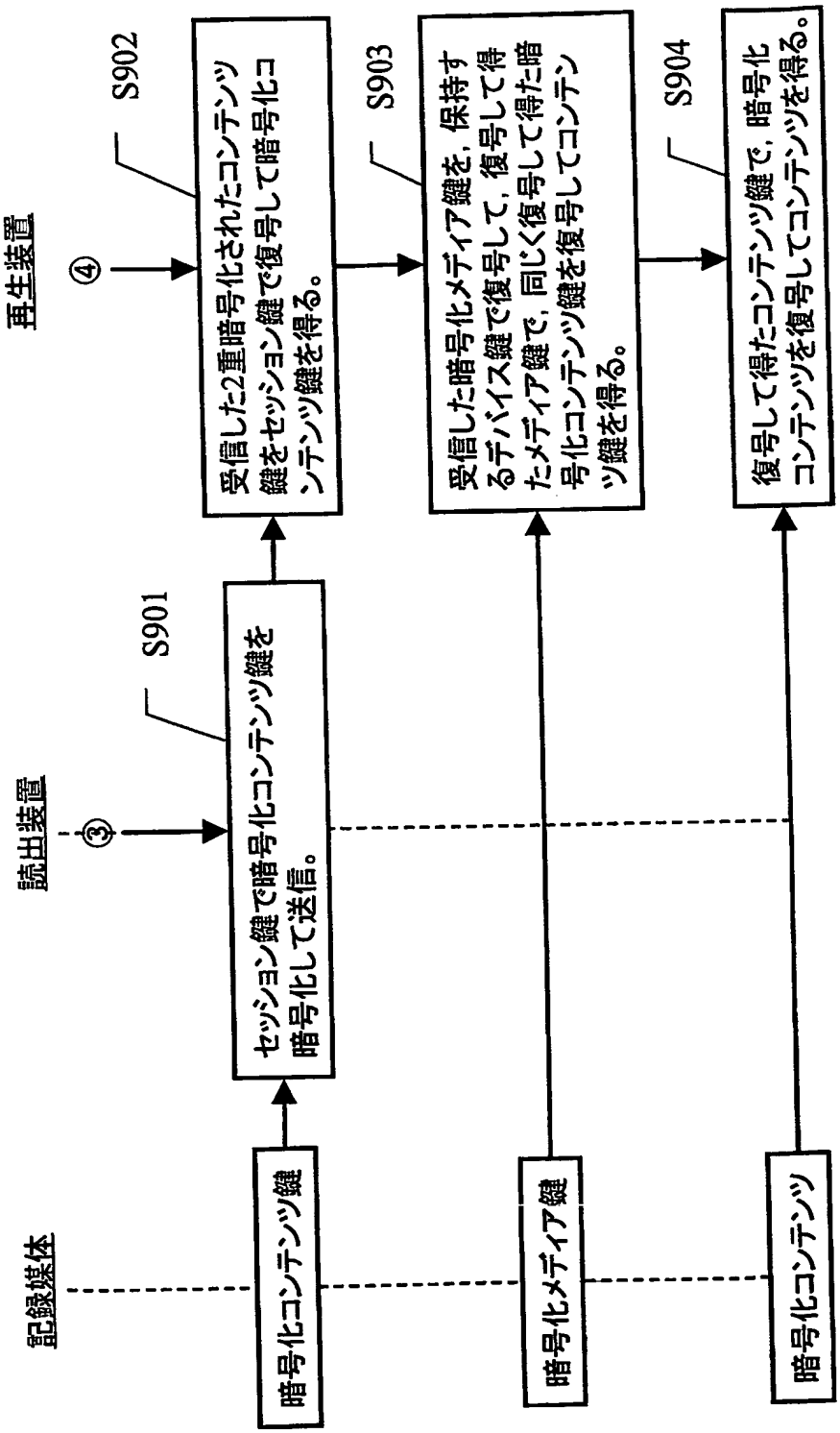
【図７】


再生装置
②
読出装置
①
S701
部分リスト、及び証明書を受信して、保持するCAの公開鍵で、受信した部分リスト、及び証明書に付与された署名を検証する。さらに、部分リストと証明書から、当該証明書が有効か否かを検証する。
S702
検証OK？
No
END
Yes
S703
保持する証明書を再生装置へ送信する。
記録媒体

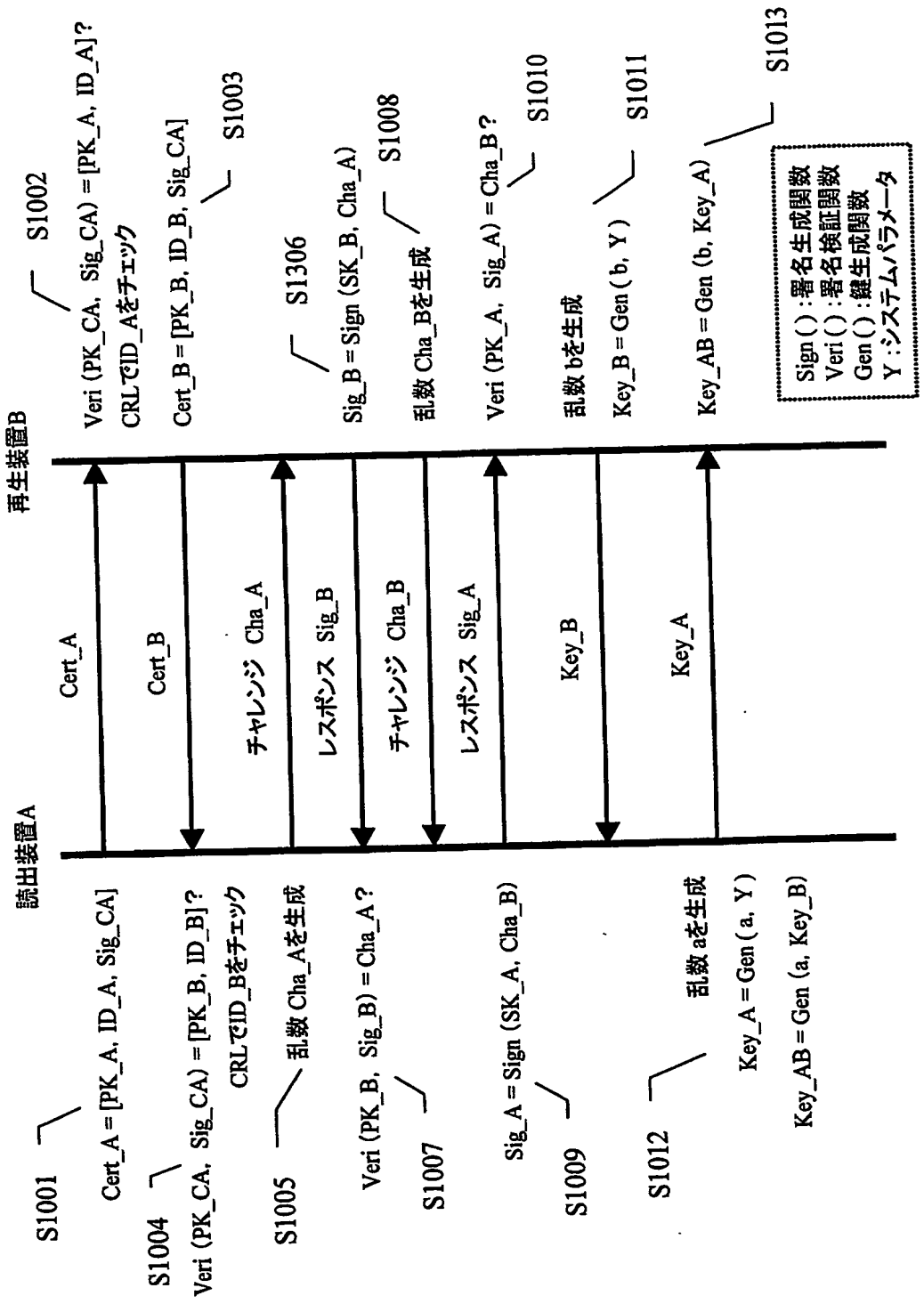
【図８】


再生装置
読出装置
記録媒体
②
③
④
S801
証明書を受信して、保持するCAの公開鍵で、受信した証明書に付与された署名を検証する。さらに、保持するリストDと、受信した証明書から、当該証明書が有効か否かを検証する。
S802
検証OK？
Yes
No
END
S803
SAC処理を実行
S804
SAC処理を実行

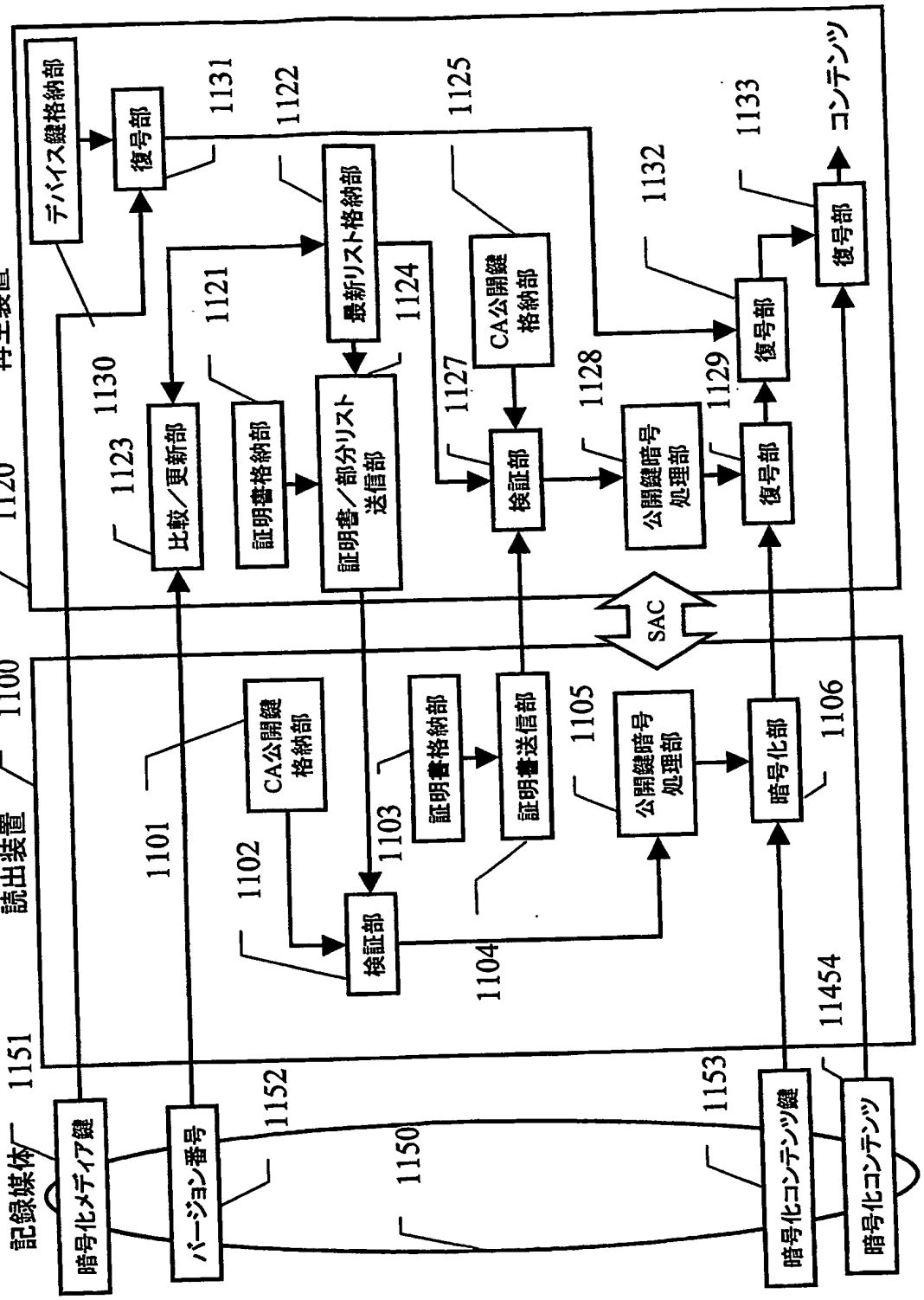
【図９】


記録媒体
読出装置
再生装置
暗号化コンテンツ鍵
暗号化メディア鍵
暗号化コンテンツ
③
④
S901
セッション鍵で暗号化コンテンツ鍵を暗号化して送信。
S902
受信した2重暗号化されたコンテンツ鍵をセッション鍵で復号して暗号化コンテンツ鍵を得る。
S903
受信した暗号化メディア鍵を，保持するデバイス鍵で復号して，復号して得たメディア鍵で，同じく復号して得た暗号化コンテンツ鍵を復号してコンテンツ鍵を得る。
S904
復号して得たコンテンツ鍵で，暗号化コンテンツを復号してコンテンツを得る。

【図１０】


読出装置A
再生装置B
S1001
Cert_A = [PK_A, ID_A, Sig_CA]
Cert_A
S1002
Veri (PK_CA, Sig_CA) = [PK_A, ID_A]?
CRLでID_Aをチェック
S1004
Veri (PK_CA, Sig_CA) = [PK_B, ID_B]?
CRLでID_Bをチェック
Cert_B
Cert_B = [PK_B, ID_B, Sig_CA]
S1003
S1005
乱数 Cha_Aを生成
チャレンジ Cha_A
S1306
Sig_B = Sign (SK_B, Cha_A)
レスポンス Sig_B
Veri (PK_B, Sig_B) = Cha_A?
S1007
チャレンジ Cha_B
S1008
乱数 Cha_Bを生成
Sig_A = Sign (SK_A, Cha_B)
S1009
レスポンス Sig_A
Veri (PK_A, Sig_A) = Cha_B?
S1010
Key_B
乱数 bを生成
S1012
乱数 aを生成
Key_A = Gen (a, Y)
S1011
Key_B = Gen (b, Y)
Key_A
Key_AB = Gen (a, Key_B)
Key_AB = Gen (b, Key_A)
S1013
Sign ( ) :署名生成関数
Veri ( ) :署名検証関数
Gen ( ) :鍵生成関数
Y :システムパラメータ

【図１１】


記録媒体
暗号化メディア鍵
バージョン番号
暗号化コンテンツ鍵
暗号化コンテンツ
1150
1151
1152
1153
11454
読出装置
1100
1101
CA公開鍵格納部
1102
検証部
1103
証明書格納部
1104
証明書送信部
1105
公開鍵暗号処理部
1106
暗号化部
SAC
再生装置
1120
デバイス鍵格納部
復号部
1131
1122
最新リスト格納部
1125
1121
比較／更新部
1123
1130
証明書格納部
証明書／部分リスト送信部
1124
1127
CA公開鍵格納部
検証部
1128
1132
公開鍵暗号処理部
1129
復号部
1133
復号部
コンテンツ

【図１２】

バージョン番号:VN	0003
(読出装置の)無効化するID:ID1	0001
(読出装置の)無効化するID:ID2	0002
(再生装置の)有効な証明書の先頭ID:ID3	0006
(再生装置の)有効な証明書の終端ID:ID4	0008
(再生装置の)有効な証明書の先頭ID:ID5	0010
(再生装置の)有効な証明書の終端ID:ID6	0012
(再生装置の)有効な証明書の先頭ID:ID7	0017
(再生装置の)有効な証明書の終端ID:ID8	9999
CAの署名	Sig1(SK_CA, VN ‖ ID3 ‖ ID4)
CAの署名	Sig2(SK_CA, VN ‖ ID5 ‖ ID6)
CAの署名	Sig3(SK_CA, VN ‖ ID7 ‖ ID8)
CAの署名	Sig(SK_CA, VN ‖ ID1 ‖ ID2 ‖ ID3 ‖ ID4 ‖ ID5 ‖ ID6 ‖ ID7 ‖ ID8 ‖ Sig1 ‖ Sig2 ‖ Sig3)

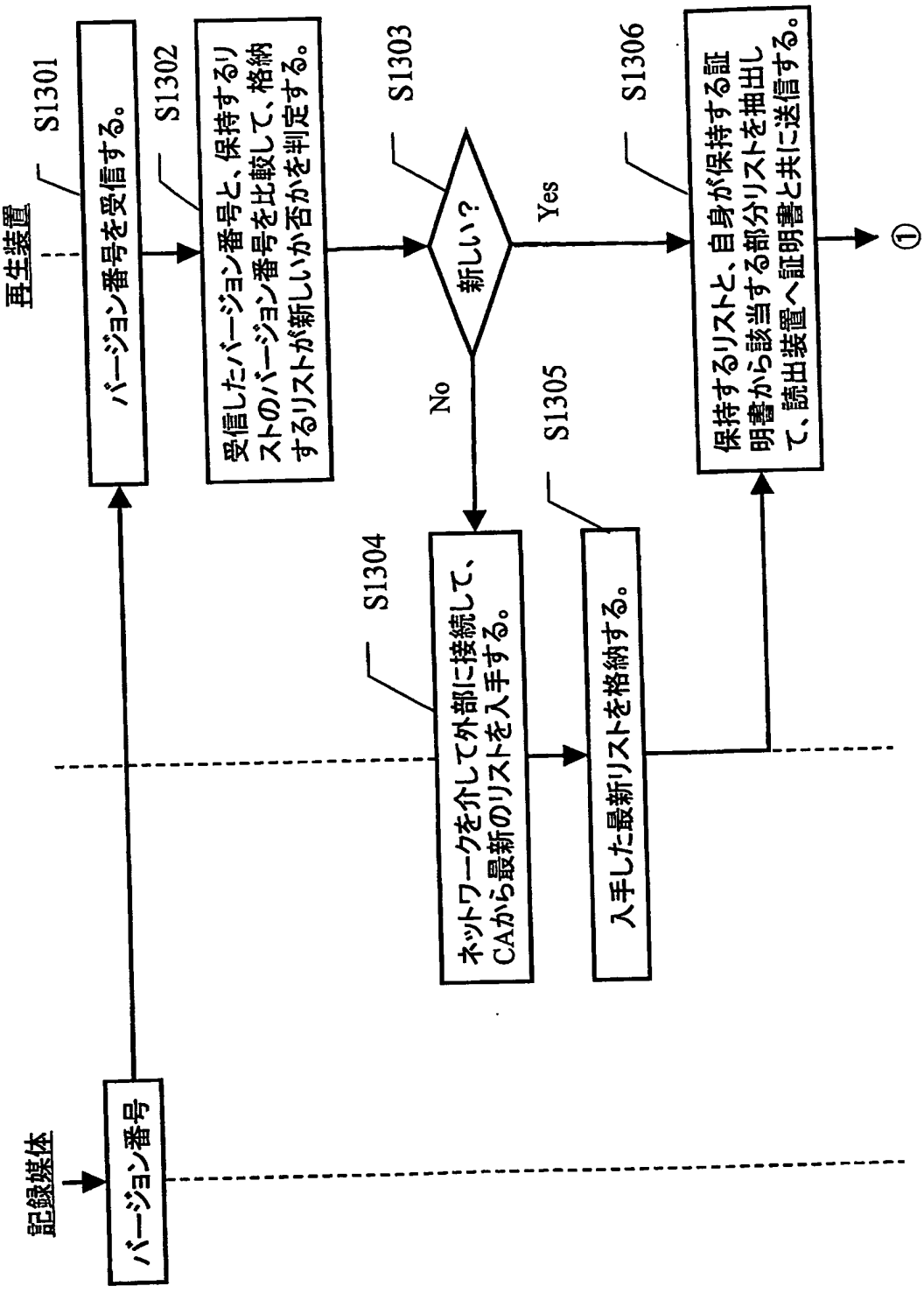
1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1210, 1211, 1212, 1213

証明書ID：1, 2, 3, 4, 5, 6, 7, 8, ×, 10, 11, 12, ×, ×, ×, ×, 17, 18, ・・・

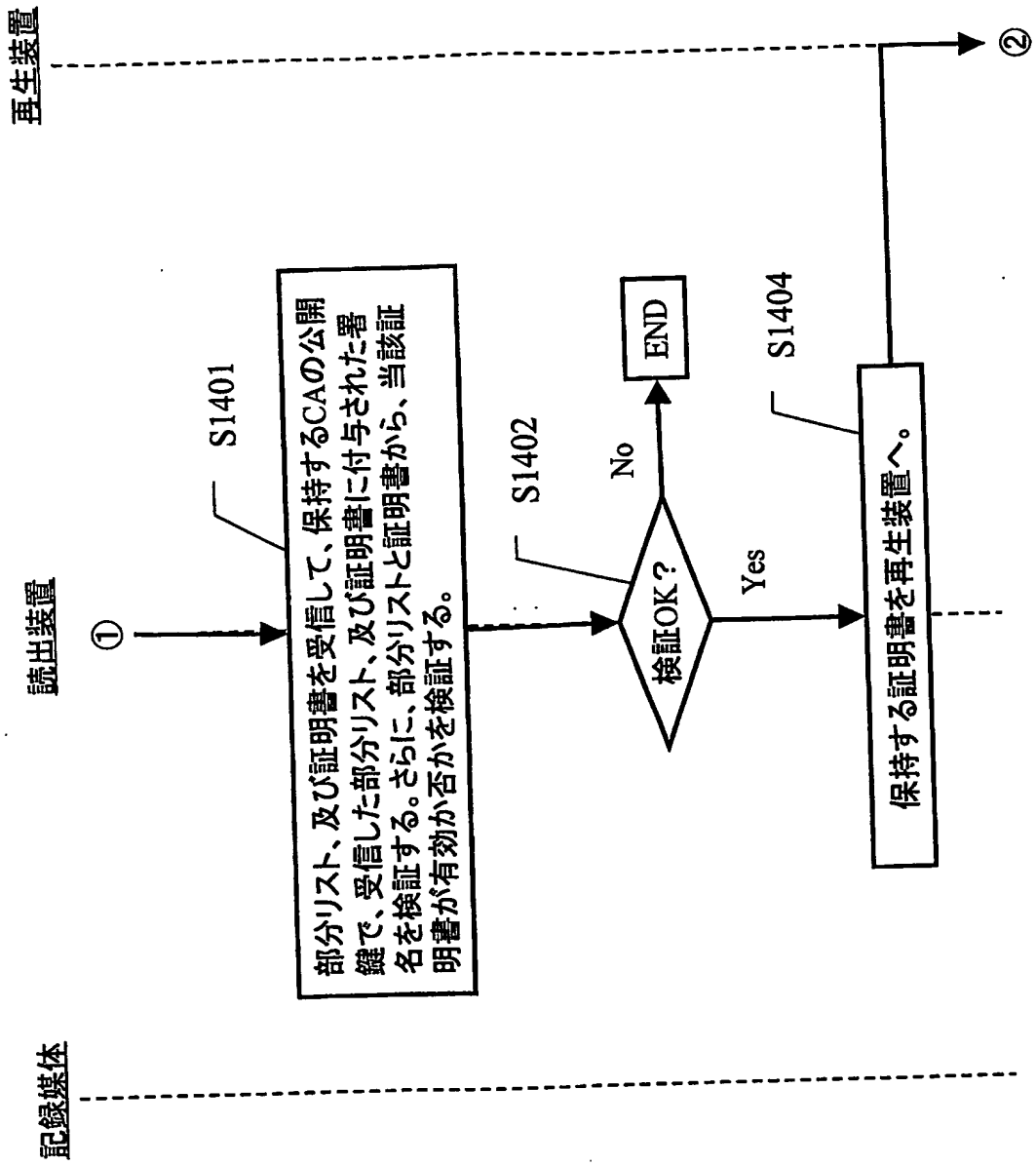
読出装置のID　　再生装置のID

×：無効化すべきID

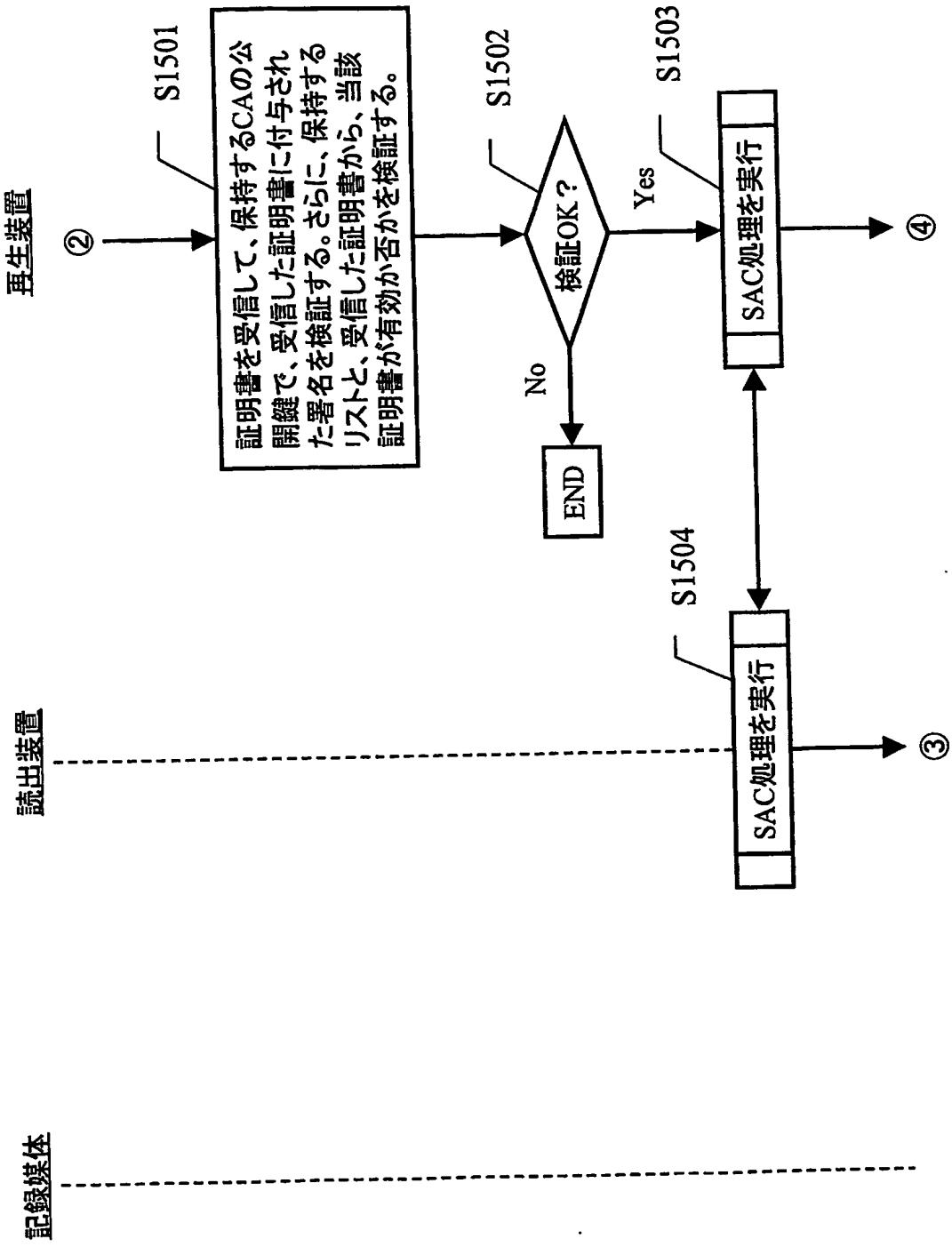
【図１３】


再生装置
S1301
バージョン番号を受信する。
S1302
受信したバージョン番号と、保持するリストのバージョン番号を比較して、格納するリストが新しいか否かを判定する。
S1303
新しい？
Yes
No
S1304
ネットワークを介して外部に接続して、CAから最新のリストを入手する。
S1305
入手した最新リストを格納する。
S1306
保持するリストと、自身が保持する証明書から該当する部分リストを抽出して、読出装置へ証明書と共に送信する。
①
記録媒体
バージョン番号

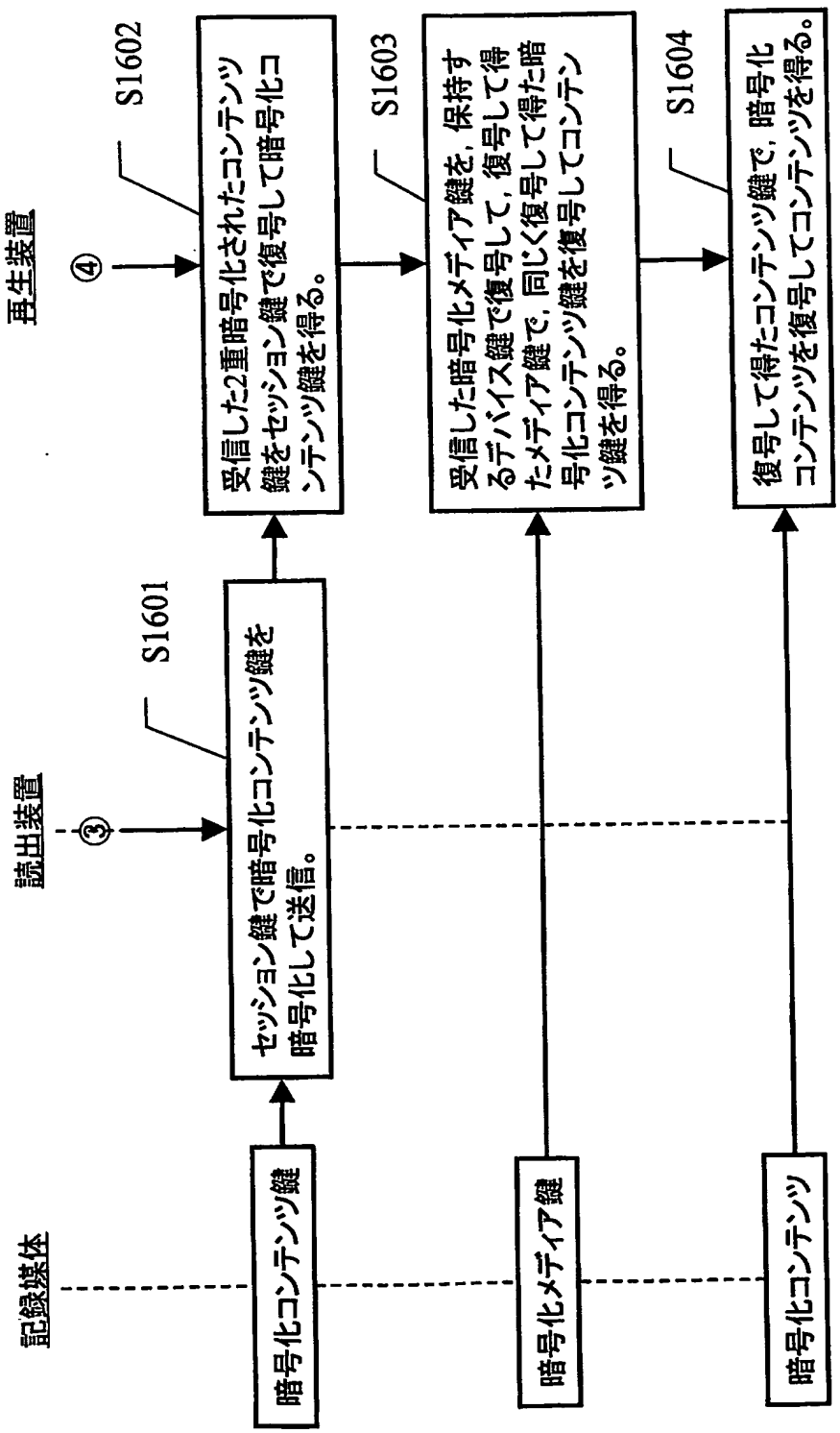
【図１４】


再生装置
読出装置
記録媒体
①
②
S1401
部分リスト、及び証明書を受信して、保持するCAの公開鍵で、受信した部分リスト、及び証明書に付与された署名を検証する。さらに、部分リストと証明書から、当該証明書が有効か否かを検証する。
S1402
検証OK?
No
END
Yes
S1404
保持する証明書を再生装置へ。

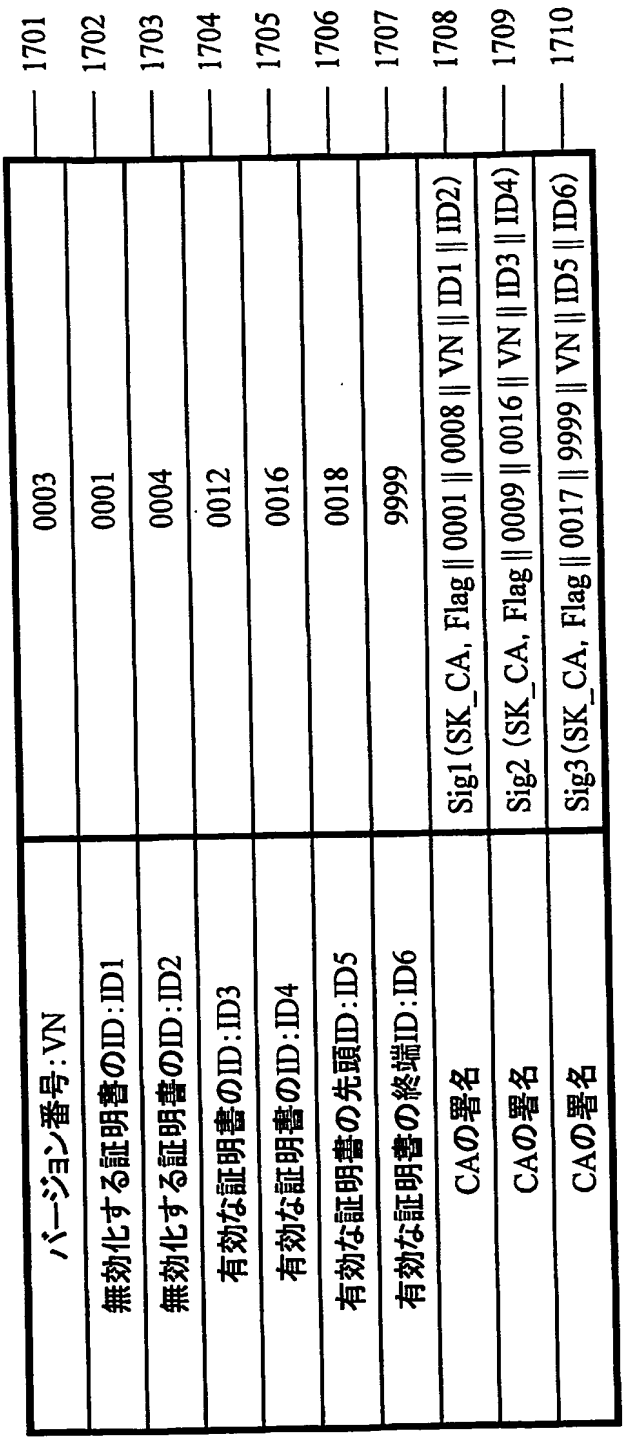
【図１５】


再生装置
読出装置
記録媒体
②
③
④
S1501
証明書を受信して、保持するCAの公開鍵で、受信した証明書に付与された署名を検証する。さらに、保持するリストと、受信した証明書から、当該証明書が有効か否かを検証する。
S1502
検証OK？
No
Yes
END
S1503
SAC処理を実行
S1504
SAC処理を実行

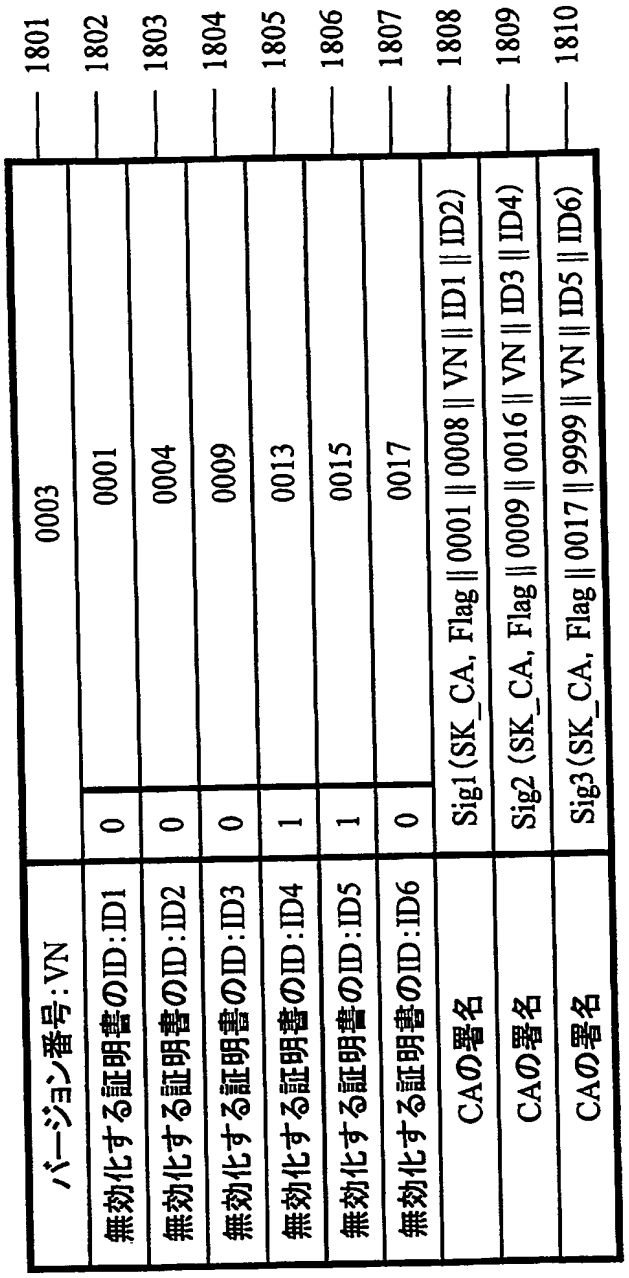
【図１６】


記録媒体
暗号化コンテンツ鍵
暗号化メディア鍵
暗号化コンテンツ
読出装置
③
S1601
セッション鍵で暗号化コンテンツ鍵を暗号化して送信。
再生装置
④
S1602
受信した2重暗号化されたコンテンツ鍵をセッション鍵で復号して暗号化コンテンツ鍵を得る。
S1603
受信した暗号化メディア鍵を，保持するデバイス鍵で復号して，復号して得たメディア鍵で，同じく復号して得た暗号化コンテンツ鍵を復号してコンテンツ鍵を得る。
S1604
復号して得たコンテンツ鍵で，暗号化コンテンツを復号してコンテンツを得る。

【図１７】


1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
バージョン番号:VN
無効化する証明書のID:ID1
無効化する証明書のID:ID2
有効な証明書のID:ID3
有効な証明書のID:ID4
有効な証明書の先頭ID:ID5
有効な証明書の終端ID:ID6
CAの署名
CAの署名
CAの署名
0003
0001
0004
0012
0016
0018
9999
Sig1(SK_CA, Flag || 0001 || 0008 || VN || ID1 || ID2)
Sig2 (SK_CA, Flag || 0009 || 0016 || VN || ID3 || ID4)
Sig3(SK_CA, Flag || 0017 || 9999 || VN || ID5 || ID6)
証明書ID：× 2, 3, × 5, 6, 7, 8, × 10, × 12, × 14, × 16, × 18, ･･･, 9999
×：無効化すべきID

【図１８】



バージョン番号:VN	0003	1801
無効化する証明書のID:ID1	0 0001	1802
無効化する証明書のID:ID2	0 0004	1803
無効化する証明書のID:ID3	0 0009	1804
無効化する証明書のID:ID4	1 0013	1805
無効化する証明書のID:ID5	1 0015	1806
無効化する証明書のID:ID6	0 0017	1807
CAの署名	Sig1(SK_CA, Flag ‖ 0001 ‖ 0008 ‖ VN ‖ ID1 ‖ ID2)	1808
CAの署名	Sig2 (SK_CA, Flag ‖ 0009 ‖ 0016 ‖ VN ‖ ID3 ‖ ID4)	1809
CAの署名	Sig3(SK_CA, Flag ‖ 0017 ‖ 9999 ‖ VN ‖ ID5 ‖ ID6)	1810

証明書ID：×2, 3, ×5, 6, 7, 8, ×10, 11, 12, ×13, ×14, ×15, 16, ×17, 18, ・・・

×：無効化すべきID

【書類名】要約書
【要約】
【課題】　公開鍵暗号を利用した認証システムにおいて、通信相手が有効か無効かを判断するためだけに用いられるリストに対しては、その入手／更新に対して強制力が働かない。
【解決手段】　再生装置が、自身の有効性を通信相手に示すリストを更新するときに、通信相手が有効か無効かを判断するためのリストも合わせて更新する。あるいは、それらリストを一体化することで、前記リストの入手／更新を強制化させる。
【選択図】　図１

特願２００３－３９４７０９

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017415

International filing date: 24 November 2004 (24.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-394709
Filing date: 25 November 2003 (25.11.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)